



**UNIVERSIDAD NACIONAL DE INGENIERÍA  
RECINTO UNIVERSITARIO SIMÓN BOLIVAR  
FACULTAD DE ELECTROTECNIA Y COMPUTACIÓN  
DEPARTAMENTO DE SISTEMAS DIGITALES Y  
TELECOMUNICACIONES.**

**MONOGRAFIA PARA OPTAR AL TÍTULO DE:  
INGENIERO ELECTRÓNICO**

**Título:**

**“Organizar Y Establecer Nuevas Soluciones de Seguridad en la Red de la  
Empresa Systems Enterprise S.A.”**

**Autores:**

- **Br. Herzan Francisco Carcache Huerta,   Carnet: 2011-37268**
- **Br. Cristian Ulises Burgos Torres,       Carnet: 2012-41142**

**Tutor: Ing. Luis Francisco López Bravo.**

**Managua, Nicaragua  
Octubre 2018**

### **Dedicatoria:**

Este esfuerzo especialmente lo queremos dedicar a todas aquellas personas que con su feroz espíritu de investigador dedicaron sus vidas para contribuir en el desarrollo pleno de la ciencia, teniendo en mente siempre como fin, el bienestar de la humanidad.

Les agradecemos profundamente por inspirarnos en el mundo del Networking todo lo que hemos aprendido y estamos por aprender, para cooperar al progreso del conocimiento científico en nuestra nación.

Muchas personas han contribuido indirecta o directamente en este estudio, razón que nos impulsa a dedicarlo también a todos los profesores de la Facultad de electrotecnia y computación nuestra universidad.

A todas las personas de nuestro país que realizan sus investigaciones para solucionar un problema que han hecho propio y que constantemente a través de cualquier medio científico intentan encontrarle una solución eficaz. Así mismo, a todas las personas que sufren las consecuencias de los pocos trabajos existentes en nuestra rama de seguridad de la información.

Por su incondicional y constante apoyo, a todos nuestros profesores, familiares y amigos, les ofrecemos este trabajo como muestra de cariño. Siempre nos inspiraron a continuar y seguir adelante hasta lograrlo ya que nunca perdimos de vista la siguiente máxima: “Si en algún momento dudas y crees que no lo logras, imagina la mirada de esperanza de aquellos que confían en ti”.

En fin, este trabajo es para todos ustedes. Nos honra poder haber hecho algo que sabemos puede generar grandes beneficios. Estamos muy felices de formar parte de ese reducido pero incansable y tenaz grupo de investigadores.

Con mucho aprecio:

Cristhian Burgos y Herzan Carcache.

### **Agradecimientos:**

En primer lugar a gracias a Dios por haberme guiado por el camino de la felicidad hasta ahora; en segundo lugar a cada uno de mi familia. Por siempre haberme dado su fuerza y apoyo incondicional que me han ayudado y llevado hasta donde estoy ahora. Agradeciéndole a mi compañero de tesis **Cristhian Burgos** por haberme ayudado en todo momento, a mis compañeros de Universidad porque en esta armonía grupal lo hemos logrado y a mi tutor monográfico quién nos ayudó en este proceso de formación, **Ing. Francisco López**.

#### **Br. Herzan Francisco Carcache Huerta.**

Primeramente, agradecerle principalmente a Dios por acompañarme a lo largo de mi carrera y guiarme a lo largo de mi aprendizaje, ayudarme en momentos de debilidad y darme la inteligencia necesaria para seguir adelante. Le doy gracias a mis padres **Héctor Burgos y Lucia Torres** por estar a mi lado y apoyarme en todo momento, por inculcarme los valores que tengo y por permitirme tener una excelente educación a lo largo de mi vida, y ser siempre el mejor ejemplo a seguir y salir adelante que tengo.

A mis hermanos **Héctor y Ana Lucia** por estar siempre a mi lado y brindarme su apoyo siempre que lo he necesitado, y ser un gran ejemplo de unidad familiar, a mis tíos **Luis y Maribel**, mis primos **Luis y Milton** por también ser una gran parte en mi vida, además de su gran apoyo en mi formación tanto como personal como profesional estando siempre presentes en todo momento y cuando más se necesitan.

A mi esposa **Meury Zamora**, la cual ha sido y será parte importante de mi vida, creyendo en mí y estando a mi lado en todo momento, demostrándome siempre su amor incondicional y paciencia. A **Herzan Carcache** por haber sido un excelente compañero de tesis y amigo, al igual que a nuestro tutor el **Ing. Francisco López** el cual siempre nos ayudó y motivo a lo largo de este camino lleno de obstáculos.

De igual manera, siempre teniendo en cuenta a una persona muy especial, que aunque ahora no está con nosotros, siempre estarás en mi mente cuando alcance grandes logros como este, Pedrito Valle.

Y por supuesto a la empresa **Sistems Enterprise S.A**, la cual nos permitió realizar esta monografía basándonos en sus instalaciones, compañeros actuales de trabajo los cuales siempre nos brindaron apoyo en momentos de duda y aprendizaje para realizar un buen trabajo monográfico.

#### **Br. Cristhian Ulises Burgos Torres.**

### **Abstract:**

In the last years, information technologies have changed the world around us, as is the case with the Internet of Things, to such an extent that information security is important to protect the confidential or private information of any business system.

In the increasing boom of the different forms of penetration or security failures that present some technologies, attackers or intruders have several abilities to collapse the computer network and the theft of information in order to obtain money in return.

Our monograph tries to implement different security equipment to protect the computer network of the company Systems Enterprise S, A. (SENCOM). With the following devices: a unified threat management that has different modules (Router, Firewall, VPN and Web Filter), an Intrusion Prevention System that acts on the basis of signatures and will be analyzing the traffic of the network towards the provider of Internet service, a Fortimail that is a mail server and at the same time is AntiSpam and finally a DNS Server.

Any type of computer threats put in risk and stability of the computer network but when implementing these security devices already mentioned, the probability that an intruder manages to steal information is significantly reduced by using the best security practices both in the entrance and in the exit.

SENCOM I need good management and administration of your resources this depends on the success of the business. Therefore, we take full advantage of all those elements that allow us to better manage the computational resources of the company and thus contribute to the achievement of the objectives we set ourselves.

This solution was viable because it allowed us to solve this problem in the company Systems Enterprise S.A. to save money and share information between different areas, is an important factor in decision making.

## Resumen:

En los últimos años las tecnologías de la información han cambiado el mundo que nos rodea como es el caso del internet de las cosas a tal punto que la seguridad informática es importante para resguardar la información confidencial o privada de cualquier sistema empresarial.

En la creciente forma de penetración o fallos de seguridad que presentan algunas tecnologías los atacantes o intrusos tienen varias habilidades para colapsar la red de computadoras con el fin del robo de la información con el fin de obtener dinero a cambio.

Nuestra monografía trata de implementar diferentes equipos de seguridad para proteger la red de computadoras de la empresa Systems Enterprise S, A. (SENCOM). Con los siguientes dispositivos: un gestión unificada de amenaza que tiene diferentes módulos (Enrutador, Firewall, VPN y Web Filter), un Sistema de Prevención de Intrusos que actúa en base a firmas y estará analizando el tráfico de la red de cara al proveedor de servicio de internet, un Fortimail que es servidor de correo y al mismo tiempo es AntiSpam y por ultimo un Servidor DNS.

Cualquier tipo de amenazas informáticas ponen en riesgos y estabilidad de la red de computadora pero al implementar estos dispositivos de seguridad ya mencionado, la probabilidad de que un intruso logre robar información se reduce notablemente al usar las mejores prácticas de seguridad tanto en la entrada como en la salida.

SENCOM necesito de la buena gestión y administración de sus recursos de esto depende el éxito del negocio. Por lo cual aprovechamos al máximo todos aquellos elementos que nos permiten gestionar de una mejor manera los recursos computacionales de la empresa y de esta forma contribuir al logro de los objetivos que nos planteamos.

Esta solución nos resultó viable porque nos permitió resolver este problema en la empresa Systems Enterprise S.A. para ahorrar dinero y Compartir información entre las distintas áreas, es un factor importante en la toma de decisión.

## Tabla de Ilustraciones:

Fig. 1.2.1 Red de Computadora antes. ....	7
Fig. 1.2.2 Esquema de la Red después de utilizar el nuevo UTM. ....	7
Fig. 1.2.3 Configuración de los enlaces WAN y LAN. ....	8
Fig. 1.2.4 Ingresando los DNS Público y DNS de Google. ....	8
Fig. 1.2.5 Configuración del Servidor de correo. ....	9
Fig. 1.3.1 Permisos del Servidor de Correo. ....	9
Fig. 1.3.2 Acceso a los protocolos HTTP, HTTPS y POP3. ....	9
Fig. 1.3.3 Enrutamiento entre las distintas VLAN. ....	10
Fig. 1.3.4 Establecimiento del NAT Dinámico. ....	10
Fig. 1.3.5 Establecimiento del Network Time Protocol. ....	11
Fig. 1.3.6 NAT Estático en el servidor de tickets y el FTP. ....	11
Fig. 1.3.7 Restricción de categoría de sitios web usando Web Blocker. ....	12
Fig. 2.2.1 Antes de la Implementación. ....	14
Fig. 2.2.2 Esquema de la implementación del sensor IPS NSP M-1450. ....	14
Fig. 2.2.3 Preparación del sensor M-1450. ....	15
Fig. 2.2.4 Conexión del sensor desde el puerto de consola. ....	15
Fig. 2.2.5 Configuración del sensor con el comando setup. ....	16
Fig. 2.2.6 Terminando de configurar con el comando setup. ....	16
Fig. 2.2.7 Establecer la llave compartida en la manager. ....	17
Fig. 2.2.8 Verificación de la llave compartida. ....	17
Fig. 2.2.9 Estableciendo la llave compartida en el sensor. ....	18
Fig. 2.2.10 Verificando la relación entre el sensor y la manager. ....	18
Fig. 2.3.1 Elegir la versión a actualizar y descargar. ....	19
Fig. 2.3.2 Actualizando la versión del IPS del NSP M-1450. ....	19
Fig. 2.3.3 Última versión disponible para el IPS NSP M-1450. ....	20
Fig. 2.3.4 Versión anterior del IPS. ....	20
Fig. 2.3.5 Implementación del IPS con sus enlaces WAN, LAN y AP. ....	21
Fig. 2.4.1 Configuración de las políticas del IPS. ....	21
Fig. 2.4.2 Asignación de las políticas a los puertos correspondientes. ....	22
Fig. 2.4.3 Guardando las políticas del IPS. ....	22
Fig. 2.4.4 Políticas de Firewall del IPS. ....	23
Fig. 2.4.5 Antes de implementar el IPS. ....	23
Fig. 2.4.6 Después de implementar el IPS. ....	24
Fig. 3.1.1 Tipos de jerarquía para un servidor DNS. ....	25
Fig. 3.1.2 Funcionamiento del Forwarders. ....	25
Fig. 3.2.1 Selección del idioma de instalación en Linux. ....	26
Fig. 3.2.2 Elección del tipo de teclado en el servidor. ....	26
Fig. 3.2.3 Establecer las Credenciales de acceso. ....	27
Fig. 3.2.4 Instalación del Sistema Operativo. ....	27
Fig. 3.2.5 Ingreso de las Credenciales. ....	28
Fig. 3.2.6 Elección de los módulos a instalar. ....	28
Fig. 3.2.7 Descarga e Instalación de los paquetes requeridos. ....	29
Fig. 3.2.8 Configuración de la interfaz Externa. ....	29
Fig. 3.2.9 Ajuste del Nombre de Dominio. ....	30
Fig. 3.2.10 Estableciendo las configuraciones realizadas. ....	30
Fig. 3.2.11 Configurando la Dirección IP del Server. ....	31
Fig. 3.2.12 Guardando los Cambios Realizados. ....	31
Fig. 3.2.13 Verificación de los módulos activados en el server. ....	32
Fig. 3.2.14 Habilitación de la cache del DNS transparente. ....	32
Fig. 3.2.15 Añadir los Forwarders de los DNS de Google. ....	33
Fig. 3.2.16 Configuración de nuestro dominio. ....	33
Fig. 3.3.1 Comprobando nuestra dirección IP en la PC. ....	34
Fig. 3.3.2 Verificación del servidor DNS. ....	34

Fig. 4.1.1 Arquitectura de implementación del Fortimail..	36
Fig. 4.2.1 Descarga del Firmware desde la página oficial de Fortinet.....	37
Fig. 4.2.2 Selección del producto el cual implementaremos.....	37
Fig. 4.2.3 Elección de la última versión disponible del Fortimail. ....	38
Fig. 4.2.4 Procediendo a descargar la última versión disponible del firmware. ....	38
Fig. 4.2.5 Descargando la versión 5.4 del Fortimail. ....	39
Fig. 4.2.6 Selección del archivo a desplegar en nuestro Hypervisor .....	39
Fig. 4.2.7 Despliegue del OVF del Fortimail para su debida instalación.....	40
Fig. 4.2.8 Selección del Firmware para el despliegue del Fortimail.....	40
Fig. 4.2.9 Elección del archivo necesario del Fortimail.....	41
Fig. 4.2.10 Especificaciones del requerimiento del Fortimail.....	41
Fig. 4.2.11 Aceptación de la licencia. ....	42
Fig. 4.2.12 Configuración del nombre de la máquina virtual.....	42
Fig. 4.2.13 Estableciendo el almacenamiento de la máquina virtual.....	43
Fig. 4.2.14 Creación del disco virtual VMDK, reservando el espacio definido. ....	43
Fig. 4.2.15 Tipo de Almacenamiento para el Fortimail. ....	44
Fig. 4.2.16 Porcentaje del despliegue de la máquina virtual del Fortimail.....	44
Fig. 4.3.1 Finalización del despliegue de la máquina virtual.....	45
Fig. 4.3.2 Arranque de la máquina virtual del Fortimail. ....	45
Fig. 4.3.3 Autenticación del Fortimail. ....	46
Fig. 4.3.4 Ingresando las Credenciales por defecto.....	46
Fig. 4.3.5 Estableciendo el direccionamiento de IP privada de nuestra Empresa. ....	47
Fig. 4.3.6 Entrando a la Interfaz Gráfica desde el Navegador.....	47
Fig. 4.3.7 Confirmando la excepción de seguridad. ....	48
Fig. 4.3.8 Ingresando las credenciales de administrador en la consola del Fortimail.....	48
Fig. 4.3.9 Acceso a la interfaz Gráfica del Fortimail.....	49
Fig. 4.4.1 Interacción con la consola del Fortimail. ....	50
Fig. 4.4.2 Elección del Archivo de Licencia para la consola. ....	50
Fig. 4.4.3 Búsqueda del archivo en nuestro ordenador.....	51
Fig. 4.4.4 Subida del archivo de licencia a la consola. ....	51
Fig. 4.4.5 Confirmación de la actualización por medio del archivo de licencia. ....	51
Fig. 4.5.1 Seleccionando el Wizard de la consola del Fortimail. ....	52
Fig. 4.5.2 Confirmando el acceso al Wizard del Fortimail. ....	52
Fig. 4.5.3 Estableciendo la nueva contraseña de acceso. ....	53
Fig. 4.5.4 Confirmando las configuraciones necesarias para el upgrade. ....	53
Fig. 4.5.5 Añadiendo los puertos de nuestro servidor de correo.....	54
Fig. 4.5.6 Añadiendo nuestro dominio y el Gateway de la IP Privada.....	54
Fig. 4.5.7 Configuración inicial del Antispam. ....	55
Fig. 4.5.8 Elección del nivel de Escaneo del Antispam. ....	55
Fig. 4.5.9 Creación de política principal de Acceso. ....	56
Fig. 4.5.10 Estableciendo el Dominio al Antispam. ....	56
Fig. 4.5.11 Estableciendo en la política de acceso y la acción a tomar de Relay. ....	57
Fig. 4.5.12 Finalizando la configuración del Wizard.....	58
Fig. 4.5.13 Resumen general de la regla de la política de acceso. ....	58
Fig. 4.5.14 Regresando con las nuevas credenciales y políticas establecida. ....	59
Fig. 4.6.1 Configuración de los perfiles.....	60
Fig. 4.7.1 Estableciendo el perfil de sesión. ....	61
Fig. 4.7.2 Creación de la política de sesión.....	61
Fig. 4.7.3 Confirmación de la política de sesión. ....	62
Fig. 4.8.1 Panel del Antispam.....	62
Fig. 4.8.2 Configuración del perfil de Antispam. ....	63
Fig. 4.8.3 Perfil del Antispam en la entrada.....	64
Fig. 4.8.4 Perfil de Salida del Antispam. ....	65
Fig. 4.8.5 Política tanto entrante como saliente.....	65
Fig. 4.8.6 Perfil de Contenido de Entrada.....	66
Fig. 4.8.7 Continuación del Perfil de contenido. ....	66

Fig. 4.8.8 Finalización del Perfil de Contenido.....	67
Fig. 4.8.9 Configuración del Antispam. ....	67
Fig. 4.8.10 Configuración de lista negra o blanca. ....	68
Fig. 4.8.11 Lista Blanca. ....	69
Fig. 4.8.12 Lista Negra.....	70
Fig. 4.9.1 Sitios Web con envíos de correo no deseado. ....	71
Fig. 5.1.1 Esquema de la Zona DMZ.....	72
Fig. 5.1.2 Esquema Antes de la implementación de la Zona DMZ.....	73
Fig. 5.1.3 Diagrama de red de SENCOM.. ....	74
Fig. 5.1.4 Primeros Pasos para la creación de la interfaz en el ESXI. ....	76
Fig. 5.1.5 Procedimiento para la creación de la interfaz. ....	76
Fig. 5.1.6 Establecimiento de la interfaz de la zona DMZ. ....	77
Fig. 5.1.7 Creando la Interfaz de la zona DMZ.....	77
Fig. 5.1.8 Configurando la zona DMZ.....	78
Fig. 5.1.9 Agregando la interfaz configurada al ESXI. ....	78
Fig. 5.1.10 Establecimiento de la interfaz del ESXI. ....	79
Fig. 5.2.1 Plataforma del UTM FortiGate 200 D para establecer la zona DMZ.. ....	79
Fig. 5.3.1 Establecimiento de los puertos del UTM con sus direccionamiento IP Privado.....	80
Fig. 5.3.2 Configuración de la interfaz LAN de SENCOM.....	80
Fig. 5.3.3 Configuración del Puerto del UTM para la Zona DMZ. ....	81
Fig. 5.3.4 Configuración del enlace WAN con su IP Publica. ....	81
Fig. 5.4.1 Integrando los Servidores Forwarding del DNS de Google.....	82
Fig. 5.4.2 Establecimiento de los servidores de DNS de Google.....	82
Fig. 5.5.1 Ingresando el Enrutamiento Estático del enlace WAN. ....	83
Fig. 5.5.2 Configurando del Enrutamiento Estático por el enlace WAN.....	83
Fig. 5.5.3 Configuración del enlace WAN con su Enrutamiento Estático. ....	84
Fig. 5.6.1 Establecimientos de las distintas políticas de la red de la Empresa SENCOM.....	84
Fig. 5.7.1 Establecimos la política de la Zona DMZ.....	85
Fig. 5.7.2 Configurando las políticas del NAT .....	86
Fig. 5.7.3 Estableciendo el SNAT para la utilización de la Zona DMZ.....	86
Fig. 5.7.4 Agregando el NAT a las políticas de la red.....	87
Fig. 5.8.1 Configuración del Fortimail de SENCOM.....	88
Fig. 5.8.2 Modo de Operación del Fortimail. ....	89
Fig. 5.8.3 Establecimiento del interfaz del Fortimail.....	89
Fig. 5.8.4 Configurando la interfaz y permitiendo los distintos protocolos de red. ....	90
Fig. 5.8.5 Estableciendo la interfaz del Fortimail. ....	90
Fig. 5.8.6 Ingresando los Servidores DNS de Google.....	91
Fig. 5.9.1 Enrutamiento Estático del Fortimail. ....	91
Fig. 5.9.2 Mostrando el enrutamiento del Fortimail.....	92
Fig. 5.9.3 Estableciendo las políticas del Fortimail.....	92
Fig. 5.9.4 Establecimiento de la política de entrada del Fortimail.....	93
Fig. 5.9.5 Establecimiento de la política de salida del Fortimail.....	93
Fig. 1A.1 Diagrama de la red SENCOM.....	i



## Lista de Acrónimos:

<b>AP:</b> Punto de Acceso	<b>ISP:</b> Internet Service Provider
<b>Bandwidth:</b> Ancho de Banda	<b>IPS:</b> Intrusion Prevention System
<b>Brute Force Attack:</b> Ataque a Fuerza Bruta	<b>IMAP:</b> Internet Message Access Protocol
<b>CSMA/CD:</b> Carrier Sense Multiple Access / Collision Detection	<b>LAN:</b> Local Area Network
<b>Domain:</b> Dominio	<b>Linux:</b> Versión Shareware y/o Freeware del conocido sistema operativo Unix
<b>DHCP:</b> Dynamic Host Configuration Protocol	<b>Packet:</b> Paquete Cantidad mínima de datos que se transmite en una red
<b>DoS:</b> Denial of Service	<b>PING Packet Internet Groper:</b> Rastreador de Paquetes Internet. Programa utilizado para comprobar si un Host está disponible
<b>DDoS:</b> Distributed Denial of Service Attack	<b>QoS:</b> Quality of Service
<b>DNS:</b> Domain Name System	<b>RAM:</b> Random Access Memory
<b>DMZ:</b> Demilitarized Zone	<b>ROM:</b> Read Only Memory
<b>Ethernet:</b> Diseño de red de área local normalizado como IEEE 802.3	<b>SMTP:</b> Simple Mail Transfer Protocol
<b>Firewall:</b> Cortina de Fuego	<b>Sniffer:</b> Pequeño programa que busca una cadena numérica o de caracteres en los paquetes que atraviesan un nodo con objeto de conseguir alguna información.
<b>GUI Graphic User Interface:</b> Interface Gráfico de Usuario	<b>Spam / Spammer:</b> Manda grandes cantidades de correo o mensajes muy largos.
<b>Hacker:</b> Experto en informática capaz de entrar en sistemas cuyo acceso es restringido	<b>SSL:</b> Secure Sockets Layer
<b>HTML:</b> HyperText Markup Language	<b>TCP:</b> Transmission Control Protocol
<b>HTTP:</b> Hypertext Transfer Protocol	<b>TFTP:</b> Trivial File Transfer Protocol
<b>HTTPS:</b> Hypertext Transport Protocol Secure	<b>Time-out:</b> Parámetro que indica a un programa el tiempo máximo de espera antes de abortar una tarea o función
<b>Header:</b> Cabecera	<b>TTL:</b> Time To Live
<b>INTERNET:</b> Conjunto de redes y ruteadores que utilizan el protocolo TCP/IP y que funciona como una sola gran red.	<b>UDP:</b> User Datagram Protocol
<b>INTRANET:</b> Se llaman así a las redes tipo Internet pero que son de uso interno	<b>UTM:</b> Unified Threat Management
<b>IEE:</b> Institute of Electrical and Electronics Engineers	<b>VoIP:</b> Voice over IP
<b>ITU:</b> International Telecommunication Union	<b>WAN:</b> Wide Area Network
<b>ISO:</b> International Organization for Standardization	

## TABLA DE CONTENIDO

DEDICATORIA: .....	II
AGRADECIMIENTOS: .....	III
ABSTRACT: .....	IV
RESUMEN: .....	V
TABLA DE ILUSTRACIONES: .....	VI
LISTA DE ACRÓNIMOS:.....	IX
TABLA DE CONTENIDO .....	X
INTRODUCCION: .....	1
OBJETIVOS: .....	2
OBJETIVO GENERAL: .....	2
OBJETIVOS ESPECÍFICOS:.....	2
ANTECEDENTES:.....	3
JUSTIFICACIÓN:.....	4
ESTRUCTURA DE CONTENIDO .....	5
CAPÍTULO 1.....	6
1. UTM .....	6
1.1. Teoría:.....	6
1.2. Implementación:.....	7
1.3. Permisos en el servidor de Correo.....	9
CAPÍTULO 2.....	13
2. IPS: .....	13
2.1. Base Teórica: .....	13
2.2. Implementación:.....	14
2.3. Actualización del IPS:.....	19
2.4. Políticas del IPS:.....	21
CAPÍTULO 3.....	25
3. SERVIDOR DNS:.....	25
3.1. Teoría:.....	25
3.2. Implementación:.....	26
3.3. Prueba del Servidor DNS:.....	34
CAPÍTULO 4.....	35
4. FORTIMAIL: .....	35
4.1. Implementación:.....	36
4.2. Instalación del Fortimail. ....	37
4.3. Administracion de Fortimail. ....	45
4.4. Aplicando licencia. ....	49
4.5. Configuración Inicial. ....	52
4.6. Creando Perfiles del Fortimail.....	59
4.7. Perfil Session. ....	60
4.8. Perfil Antispam. ....	62
“Organizar Y Establecer Nuevas Soluciones de Seguridad en la Red de la Empresa Systems Enterprise S.A.”	X

4.9. SURBI .....	71
<b>CAPÍTULO 5.....</b>	<b>72</b>
5. DMZ .....	72
5.1. Teoría.....	72
5.2. Fortigate: .....	79
5.3. Interfaces:.....	80
5.4. Servidores DNS:.....	82
5.5. Rutas estáticas:.....	83
5.6. Políticas: .....	84
5.7. Salida DMZ:.....	85
5.8. Fortimail: .....	88
5.9. Routing: .....	91
<b>CONCLUSIONES.....</b>	<b>94</b>
<b>BIBLIOGRAFÍA: .....</b>	<b>95</b>
<b>ANEXOS: .....</b>	<b>I</b>
<b>ANEXO 1. DIAGRAMA FINAL DE SENCOM .....</b>	<b>I</b>
<b>ANEXO 2. TABLA DE COTIZACIONES .....</b>	<b>II</b>



## INTRODUCCION:

La Empresa Systems Enterprise S.A (SENCOM), ubicada en el KM 6.5 carretera norte especializada en áreas de telecomunicaciones y sistemas especiales o de bajo voltaje (centrales telefónicas, cableado estructurado, networking, seguridad electrónica, seguridad de la información, planta externa, centro de datos y energía), cuenta con una red interna protegida por un UTM (Unified Threat Management o Gestión de amenaza unificada) de cara a internet, el cual tiene módulos de IPS, Enrutador, FireWall, VPN y web filter, siendo este por el momento el único equipo en el perímetro, protegiendo los distintos servicios, aplicaciones y equipos localizados en la red interna de la empresa.

El siguiente protocolo tiene como objeto el organizar y establecer nuevas soluciones de seguridad en la red de la Empresa Systems Enterprise S.A. con la finalidad de mejorar la seguridad informática. La Empresa cuenta con un dispositivo de seguridad en la red, pero implementaremos nuevos servicios por lo que es necesario estas nuevas soluciones de seguridad, requiriendo una seguridad informática más robusta capaz de defender la red de computadoras de cualquier amenaza informática. Se emplearán las mejores prácticas de seguridad informática en la red para estar en la vanguardia en las tecnologías de la información.

La protección de los distintos servicios y aplicaciones presentes en la empresa nos ayudara a la escalabilidad como protección de futuros servicios a implementar como son: antispam, DNS, de igual manera la implementación de una zona desmilitarizada (DMZ) aislada de nuestra red interna, finalmente organizar la estructura de la red de datos de acuerdo con las necesidades de la Empresa Systems Enterprise S.A.

La Empresa Systems Enterprise S.A. proporciona Soporte Técnico a diferentes empresas en el ámbito de seguridad informáticas, resguardando todo tipo de información confidencial, reduciendo riesgo de amenazas y complejidad en la red, dentro de las nuevas implementaciones interna es aumentar la eficiencia en la seguridad de nuestra red emplearemos un IPS del cual estará de cara a internet siendo el primer analizador de tráfico en nuestro perímetro comparando firmas.

El Antispam estará protegiendo nuestro servidor de correo, analizando e implementando políticas para el tráfico dirigido a este y por ultimo nuestra zona DMZ estará conectada a nuestro UTM y a la vez aislada de nuestra red interna.

## **Objetivos:**

### ***Objetivo General:***

- Establecer las buenas prácticas de seguridad informática de la red de computadora de la Empresa Systems Enterprise S.A.

### **Objetivos Específicos:**

- Implementar el sistema de prevención de intrusos y gestión unificada de amenazas con sus debidas configuraciones para el bloqueo de las vulnerabilidades en el perímetro de la red.
- Instalar y configurar un servidor DNS.
- Implementar un analizador de correos Antispam “**Fortimail**” para la eliminación de correo no deseado para la Empresa Systems Enterprise S.A.
- Emplear un sistema de red DMZ (Zona Desmilitarizada) en la empresa Systems Enterprise S.A. (SENCOM).
- Establecer las buenas prácticas en la configuración de los dispositivos de seguridad (IPS, Antispam) con sus debidas políticas tanto de entrada como de salida.

### **Antecedentes:**

En el transcurso de los años la Empresa Systems Enterprise S.A. Ha conestado con un UTM, resguardando la seguridad de la red funcionando de la mejor manera sin haber algún incidente, pero cabe destacar que se quiere añadir nuevos servicios como es el servidor DNS que anteriormente estaba tercerizado. Por lo tanto, estos servicios requieren protección de un sistema de prevención de intrusos que estará de cara al ISP (Proveedor de Servicios de Internet) y un Fortimail que actúa como antispam y servidor de correo previniendo el contenido de spam tanto de entrada como de salida de la red, de la misma manera protegiendo nuestro DNS el cual también será implementado y es una necesidad en proteger los activos de la Empresa.

Por eso la importancia en tener los dispositivos de seguridad en la red bien concebida y efectiva que pueda proteger la inversión y los recursos de información de la Empresa Systems Enterprise S.A. Vale la pena implementar dispositivos de seguridad si los recursos y la información merecen protegerse. En la red de nuestra empresa tenemos información delicada y documentos importantes en el área administrativa; esto debe protegerse del acceso indebido.

La tecnología va presentando mejoras significativas en dispositivos y soluciones. La empresa Systems Enterprise S.A. cuenta con equipos cuyo acoplamiento a las nuevas tecnologías y estándares requieren mejorarse, por lo que encontramos como única solución, organizar y establecer soluciones de seguridad usando los equipos existentes junto con nuevos, lo que permitirá en tener un sistema de red con criterios técnicos de escalamiento, seguridad, disponibilidad e integridad de acuerdo a estándares establecidos.

Consideramos que en la Facultad de Electrotecnia y Computación de la Universidad Nacional de Ingeniería del Recinto Universitario Simón Bolívar no habido ningún tema monográfico relacionado al nuestro. Nosotros nos basamos en el libro: *Ataques en redes de datos IPV4 e IPV6*. De los autores: García Rambla, Juan Luis. Publicado en el año (2017). En España su tercera edición revisada y ampliada. En este documento se nos presenta los diferentes métodos de vulnerabilidad en el mundo del networking para establecer soluciones de seguridad.

### Justificación:

Actualmente la Empresa Systems Enterprise, cuenta con una red alámbrica e inalámbrica que proporciona soporte técnico a diferentes empresas en el ámbito de seguridad informática. El personal de esas empresas usan el internet con fines de trabajo pero algunos hacen mal uso, ingresando a sitios web para descargar recursos de origen desconocidos que pueden ocasionar que un virus informático dañe los equipos o la red, esto provocaría que los encargados en brindar el soporte técnico tengan que estar continuamente dándole mantenimiento a los dispositivos. Además el ancho de banda se ve afectado. Sin embargo, la empresa Systems Enterprise requiere mejorar la infraestructura de la red (interna) para la calidad de sus servicios.

La Empresa SISTEMAS ENTERPRISE S.A, ve necesario organizar y establecer nuevas soluciones de seguridad en la red en el perímetro interno como (IPS) y la nueva implementación de equipos de seguridad antispam (FORTIMAIL), de igual manera la nueva utilización de un servidor DNS.

De esta manera nosotros podemos dar solución a esta necesidad por separado:

- **Seguridad:** Al incorporar estos: IPS, Antispam, se tendrá una seguridad sólida en el perímetro de nuestra red, analizando todo tipo de tráfico entrante y saliente hacia el internet.
- **Establecimiento:** Los servicios actuales y los nuevos que implementaremos se ordenarán en una zona DMZ para aislar e intensificar la seguridad en el perímetro debido al contenido y reducir costos.

Esta solución, es viable porque nos permitirá resolver la problemática en nuestra empresa acerca de las vulnerabilidades de seguridad en la red informática. Lo que lleva al ahorro de dinero, a la facilidad de comunicación y poder compartir información de forma segura. Durante nuestra formación académica, asignaturas como Redes de Computadoras y Redes Telefónicas nos brindaron conocimientos sobre el amplio mundo de las tecnologías de la información y el Networking. También otras clases como metodología de la investigación, inglés, redacción técnica, Programación y Electrónica Digital. Todos estos conocimientos adquiridos en estas asignaturas nos serán útiles para el desarrollo de esta monografía.



## **Estructura de Contenido**

Esta Monografía está estructurado de la siguiente manera. En el Capítulo 1, Implementaremos la gestión unificada de amenaza. En el Capítulo 2 abordaremos la implementación del Sistema de prevención de intruso con sus respectivas políticas, base teórica y la colocación de este dispositivo de seguridad en el Rack. En el Capítulo 3 implementaremos en una máquina virtual la instalación de un servidor DNS en Linux con sus debidas configuraciones para la traducción de los distintos nombres de dominios. En el Capítulo 4 Instalaremos un Fortimail luego de haber descargado desde la página oficial de Fortinet el sistema operativo lo desplegamos en nuestro ESXI, procedemos a instalar y configurar el Fortimail. En el Capítulo 5 Creación de una zona DMZ utilizando un UTM de la marca Fortinet con su modelo FortiGate 200D y esta zona implementaremos el Fortimail.

## Capítulo 1

### 1. UTM

#### 1.1. Teoría:

Gestión Unificada de Amenazas. Nuestro UTM tiene los siguientes módulos o funcionalidades como son:

- Función de un firewall.
- Función de VPN (para hacer túneles o redes privadas).
- Filtrado de contenidos (para el bloqueo de sitios no permitidos mediante categorías).
- Sistema de Prevención de Intrusos (IPS).
- Enrutador.

**Web Filter o Filtrado de contenido:** Es un software que examina páginas web para determinar partes o totalidad de información para mostrar al usuario. Este filtro comprueba el origen o el contenido de HTML (lenguaje de marcas de hipertexto) contra una lista de reglas proporcionadas por la empresa o persona que ha instalado el filtro Web. Un filtro permite a una empresa o usuario individual bloquear páginas de sitios Web que incluyan publicidad, contenido pornográfico, spyware, virus y etc. Los vendedores de filtros Web afirman que sus productos reducirán los lapsos de tiempos en la navegación recreativa por internet entre los empleados y protegerán las redes de varias amenazas que provienen de la Web.

**VPN:** Es una conexión cifrada entre redes privadas a través de una red pública, como Internet. En vez de usar una conexión dedicada de capa 2, como una línea arrendada, una VPN usa conexiones virtuales llamadas “túneles VPN”, que se enrutan a través de Internet desde la red privada de la empresa hasta el host del sitio o del empleado remoto.

**VPN de acceso remoto:** Si se utiliza una VPN de sitio a sitio para conectar redes enteras, la VPN de acceso remoto admite las necesidades de los empleados a distancia, de los usuarios móviles y del tráfico de extranet de cliente a empresa. Una VPN de acceso remoto se crea cuando la información de VPN no se configura de forma estática, pero permite el intercambio dinámico de información y se puede habilitar y deshabilitar.

## 1.2. Implementación:

Anteriormente el UTM XTM-330 de la marca WatchGuard estaba resguardando la red de computadora ahora reemplazamos por una nueva versión del mismo fabricante UTM M200 de la misma Compañía, también en el capítulo 5 implementaremos otro UTM de la marca Fortinet la versión FortiGate 200 D para la creación de la zona DMZ usando un servidor Virtual un Fortimail.

En la Fig. 1.2.1, observamos cómo estaba nuestra red.

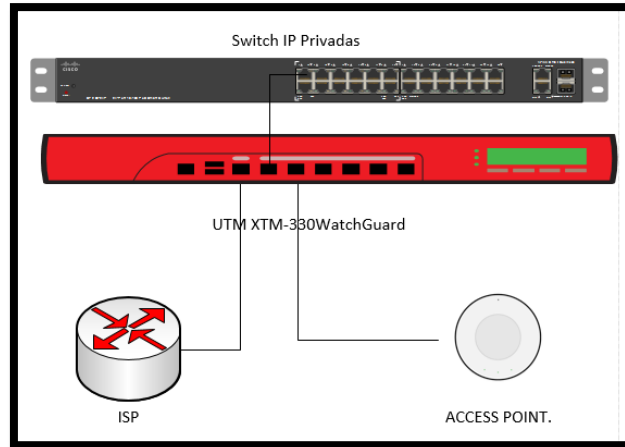


Fig. 1.2.1 Red de Computadora antes.

Después de haberse vencido el modelo XTM-330 que es una versión desfasada al modelo M200 con mejores requerimientos y características.

En la siguiente Fig.1.2.2, mostramos el esquema de la red después de utilizar el UTM.

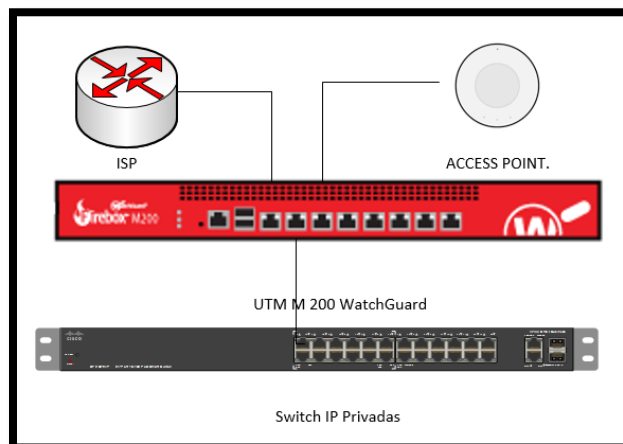


Fig. 1.2.2 Esquema de la Red después de utilizar el nuevo UTM.

Para administrar el Watchguard tiene un método muy interesante que hay que descargar un software desde la página oficial del proveedor de ese modo se puede configurar este UTM. [1]

Ponemos nuestro Gateway por defecto en status las credenciales son readonly y de admin es readwrite, las credenciales de admin son para guardar los cambios hechos en el equipo. Después de cambiar las credenciales, entramos a la parte de Network y configuramos el enlace WAN e ingresamos nuestro Gateway que es 192.168.119.2.

En la Fig.1.2.3, presentamos la configuración de los enlaces WAN y LAN del UTM.

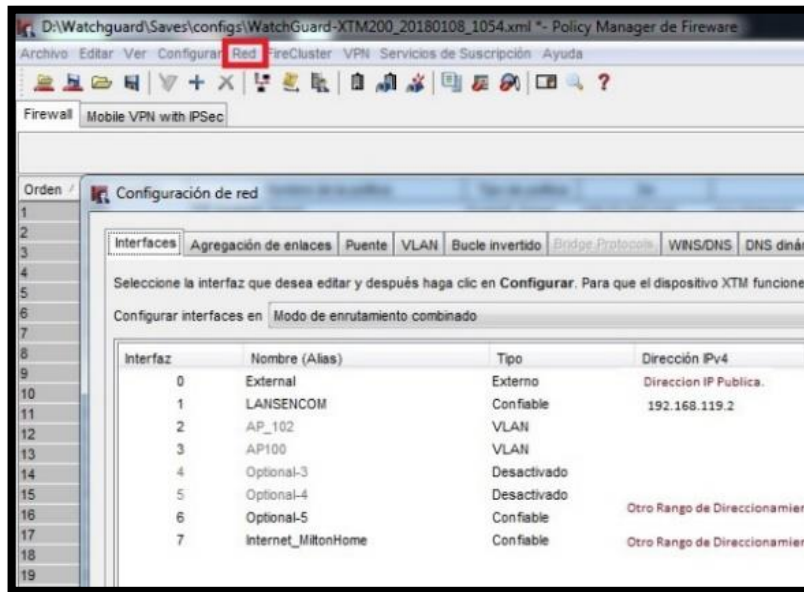


Fig. 1.2.3 Configuración de los enlaces WAN y LAN.

En la Fig.1.2.4, observamos el ingreso de los DNS Público y DNS de Google.

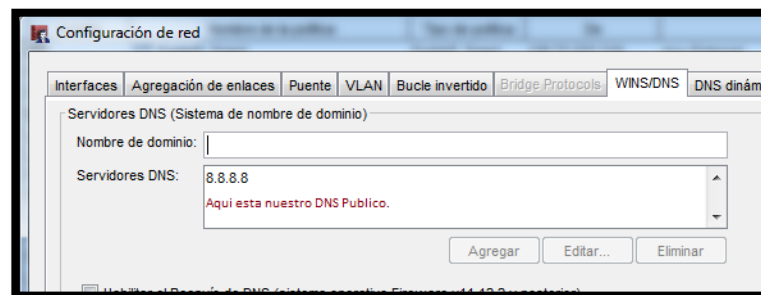


Fig. 1.2.4 Ingresando los DNS Público y DNS de Google.

En nuestro dispositivo de seguridad que es el WatchGuard establecemos la configuración del servidor de correo con su respectivo puerto como una lista de acceso. [3]

A continuación en la Fig.1.2.5, mostramos la configuración del servidor de correo.

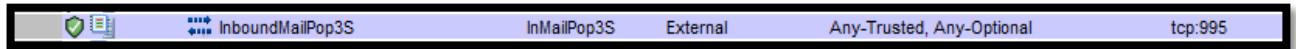


Fig. 1.2.5 Configuración del Servidor de correo.

### 1.3. Permisos en el servidor de Correo.

En la Fig.1.3.1, presentamos los permisos necesarios del servidor de correo.



Fig. 1.3.1 Permisos del Servidor de Correo.

Después de permitir con una lista de acceso tanto el POP3 que almacena el correo en un servidor remoto, HTTPS y HTTP que son los Protocolo de navegación tanto segura con sus puertos 443 y 8080. [9]

En la Fig.1.3.2, mostramos el acceso de los distintos protocolos HTTP, HTTPS y POP3.

29	HTTP-FB-Permitido	HTTP-proxy	Any-Trusted	Any-External	tcp:80
30	HTTP-proxy-Sencom01	HTTP-proxy	Any-Trusted	Any-External	tcp:80
31	POP3-proxy-Sencom01	POP3-proxy	Any-Trusted, Any-Op	Any-External	tcp:110
32	HTTPS-FB-Permitido	HTTPS-proxy	Any-Trusted	Any-External	tcp:443
33	HTTPS-proxy-Sencom01	HTTPS-proxy	Any-Trusted	Any-External	tcp:443

Fig. 1.3.2 Acceso a los protocolos HTTP, HTTPS y POP3.

En la Fig.1.3.3, observamos el enrutamiento entre las distintas VLAN.

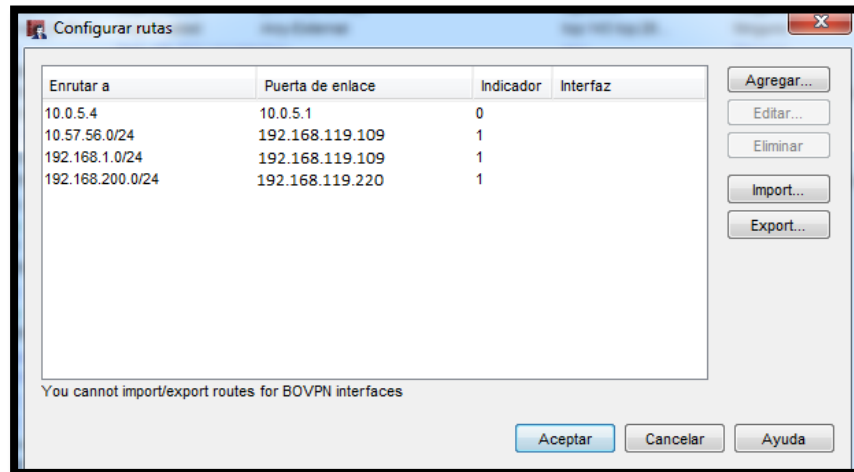


Fig. 1.3.3 Enrutamiento entre las distintas VLAN.

En nuestro dispositivo de red utilizamos (NAT Dinámico) que es la traducción de direcciones de red por lo cual una IP pública es traducida a varias IP privadas como se ve en la Fig.1.3.4, [17]

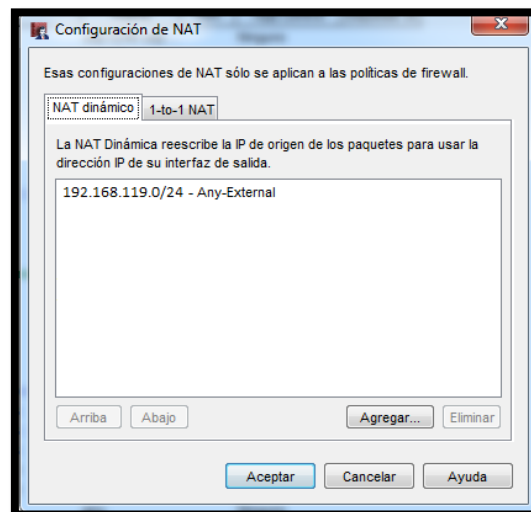


Fig. 1.3.4 Establecimiento del NAT Dinámico.

En la Fig. 1.3.5, presentamos el ingreso de nuestro protocolo de tiempo de red (NTP) al UTM para sincronizar los relojes de los sistemas informáticos.

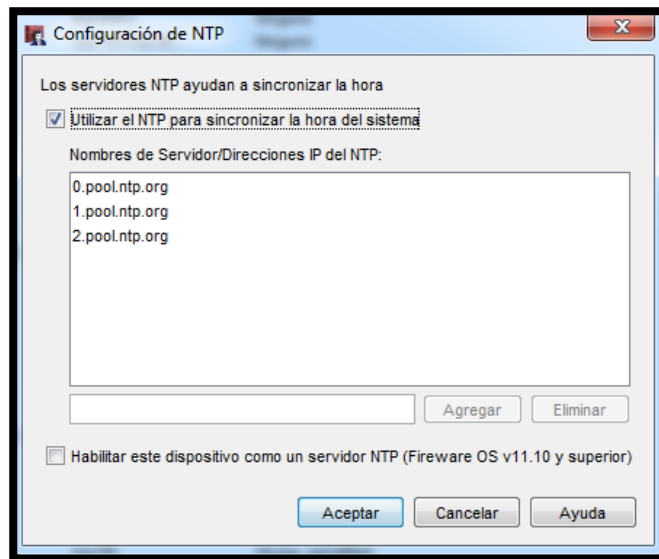


Fig. 1.3.5 Establecimiento del Network Time Protocol.

El SNAT es cuando una laptop envía un paquete desde una red a un puerto en una interfaz externa u opcional, SNAT cambia la dirección IP de destino a una dirección IP y un puerto detrás del Firewall. Si una aplicación de software utiliza más de un puerto y los puertos se seleccionan en forma dinámica, debe usar 1 a 1 NAT o verificar si un proxy en el Firebox gestiona este tipo de tráfico. Esto implica que el NAT también opera sobre las conexiones desde las redes que su Firebox protege. [16]

En la Fig. 1.3.6, mostramos la configuración del NAT Estático (SNAT) para nuestro servidor de Tickets y el FTP.

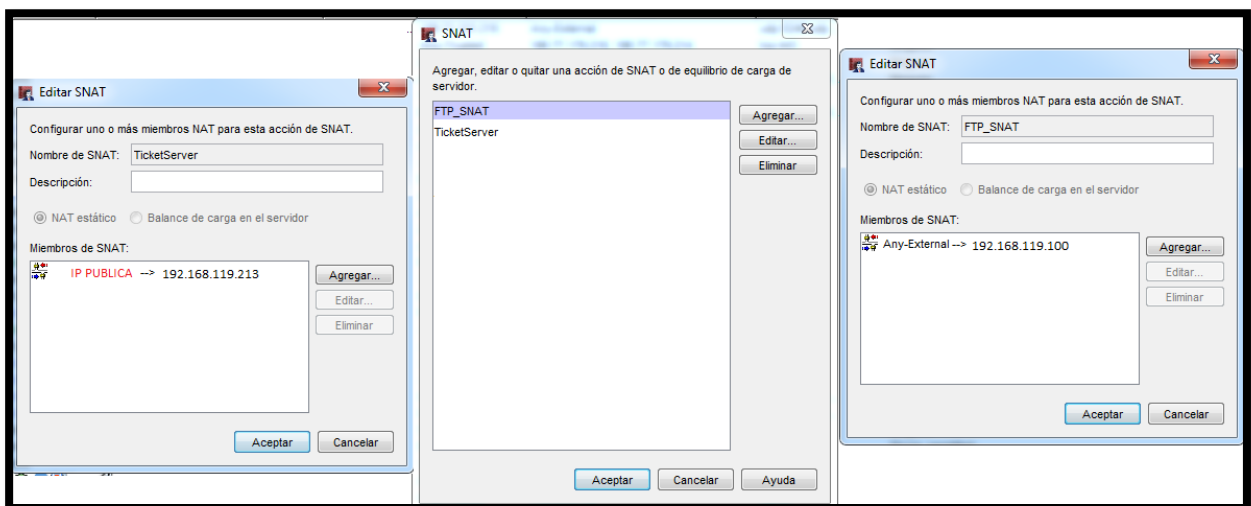


Fig. 1.3.6 NAT Estático en el servidor de tickets y el FTP.

Web blocker es el encargado de bloquear los sitios web por categoría. El objetivo es crear tantas listas negras de acceso prohibido y listas blancas de acceso permitido utilizando cualquier navegador: Internet Explorer, Mozilla Firefox, Chrome, Safari u Opera. Con el objetivo que nuestra red tenga mayor protección.

En la Fig. 1.3.7, observamos la restricción de categoría de sitios web en nuestro Web Blocker del UTM lo que deseamos bloquear en nuestra red para mayor seguridad en nuestro perímetro.

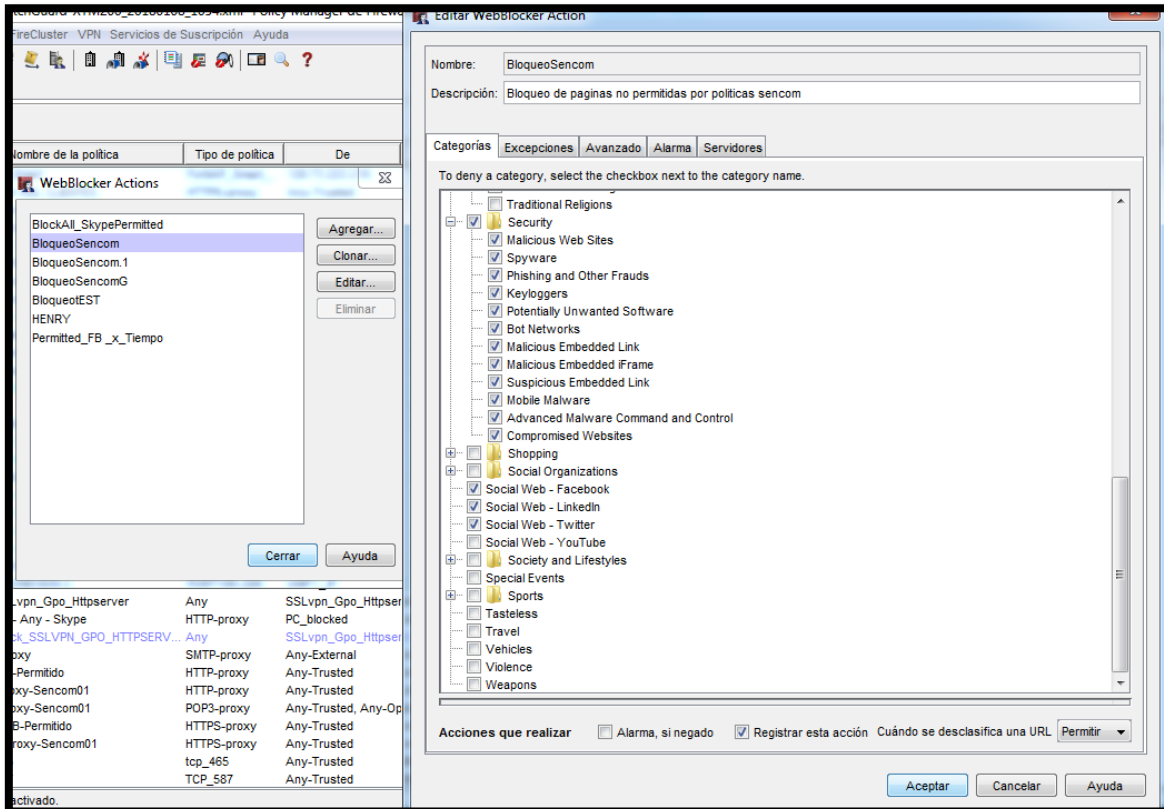


Fig. 1.3.7 Restricción de categoría de sitios web usando Web Blocker.



## Capítulo 2

### 2. IPS:

#### 2.1. Base Teórica:

Un sistema de prevención de intruso es el que examina los flujos de tráfico de la red para explotar las vulnerabilidades. Estas vulnerabilidades provienen en formas de entradas malintencionadas a una aplicación o servicio de destino que los atacantes usan para interrumpir para obtener el control de una PC. Después de un ataque exitoso el intruso puede deshabilitar la aplicación de destino, obtiene una conexión de extremo a extremo, resultando un estado de denegación de servicio, accediendo a todos los derechos y permisos disponibles.

Los IPS detectan el tráfico malintencionado en distintas formas:

**Detección basada en firmas:** funciona parecido como un antivirus y el administrador tiene que verificar que la firma este actualizado. Es decir la firma es capaz de reconocer una determinada cadena de bytes o patrón y a su vez manda una alerta.

**Detección basada en políticas:** el administrador de la red tiene que especificar que host tienen acceso a los recursos de la compañía por lo cual estas políticas de seguridad tienen que estar bien declaradas.

**Detección basada en anomalías:** este método consiste en el comportamiento anormal en nuestro sistema porque después de cierto tiempo de estar analizando el tráfico se genera un patrón luego cuando difiere activa las alarmas y esto tiende como un falso positivo.

## 2.2. Implementación:

Antes la Empresa Systems Enterprise S.A. estaba estructurada de la siguiente manera:

En la Fig. 2.2.1, presentamos como estaba la red antes de implementar el IPS.

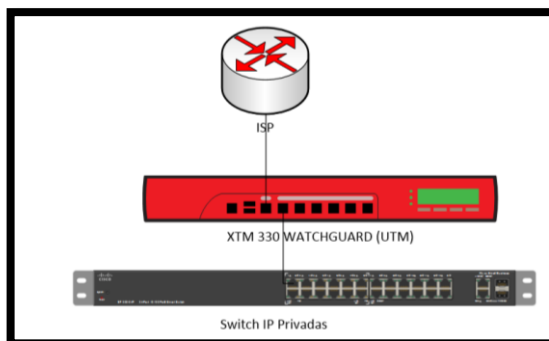


Fig. 2.2.1 Antes de la Implementación.

Procedimos a interceptar el tráfico entre el proveedor de servicios de internet y nuestro UTM WatchGuard modelo XTM 330 fue reemplazado por la versión M200 de la misma marca.

En la Fig. 2.2.2, mostramos el esquema que implementamos para el IPS.

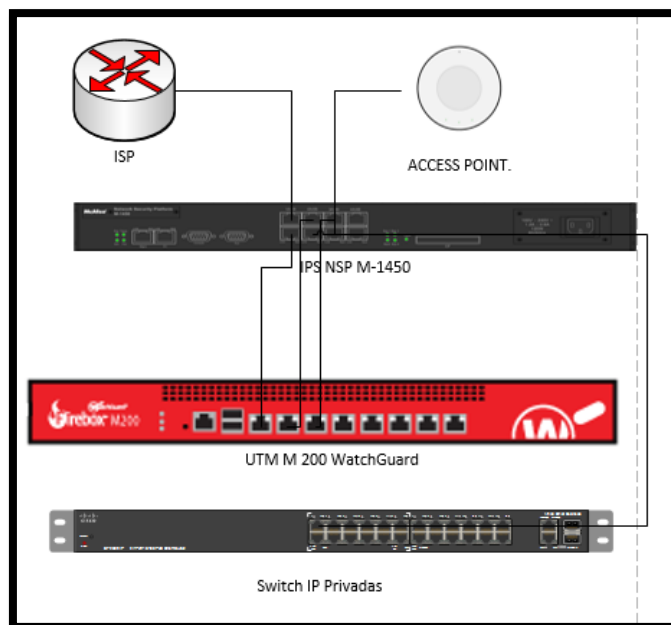
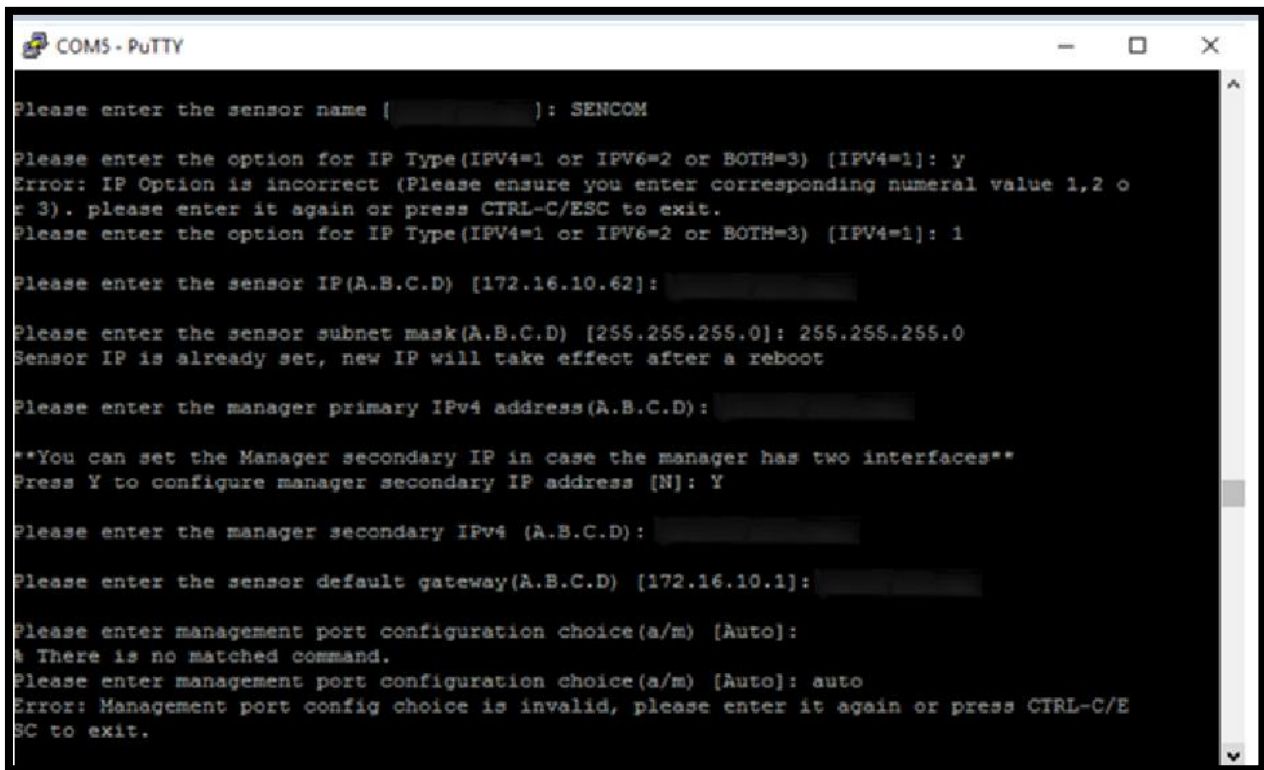


Fig. 2.2.2 Esquema de la implementación del sensor IPS NSP M-1450

Primero el sensor M-1450 tenemos que establecer la conexión con la manager del IPS. Nosotros conectamos al puerto de consola del sensor con un adaptador DB9



En la Fig. 2.2.5, enseñamos la configuración del sensor con el comando setup.



```
COMS - PuTTY

Please enter the sensor name ( ): SENCOM

Please enter the option for IP Type(IPV4=1 or IPV6=2 or BOTH=3) [IPV4=1]: Y
Error: IP Option is incorrect (Please ensure you enter corresponding numeral value 1,2 or 3). please enter it again or press CTRL-C/ESC to exit.
Please enter the option for IP Type(IPV4=1 or IPV6=2 or BOTH=3) [IPV4=1]: 1

Please enter the sensor IP(A.B.C.D) [172.16.10.62]: 
Please enter the sensor subnet mask(A.B.C.D) [255.255.255.0]: 255.255.255.0
Sensor IP is already set, new IP will take effect after a reboot

Please enter the manager primary IPv4 address(A.B.C.D): 

**You can set the Manager secondary IP in case the manager has two interfaces**
Press Y to configure manager secondary IP address [N]: Y

Please enter the manager secondary IPv4 (A.B.C.D): 

Please enter the sensor default gateway(A.B.C.D) [172.16.10.1]: 

Please enter management port configuration choice(a/m) [Auto]: 
There is no matched command.
Please enter management port configuration choice(a/m) [Auto]: auto
Error: Management port config choice is invalid, please enter it again or press CTRL-C/ESC to exit.
```

Fig. 2.2.5 Configuración del sensor con el comando setup.

La dirección del sensor 192.168.1.221 y la máscara es: 255.255.255.0. Introducimos la dirección de la manager es 192.168.1.182. La primaria y la secundaria sería la misma sino hay otra y el default Gateway es 192.168.1.1 y le damos enter. [11]

En la Fig. 2.2.6, mostramos lo última configuración del comando setup:

```
Sensor configuration is almost complete. The final step is to establish a secure management channel (trust) between the sensor and its Manager. This is accomplished by a secret key that is shared by the Manager and this sensor. Please ensure that a shared secret key has already been defined on the Manager for this sensor... Press Y to set shared secret key now or N to exit [Y]: _
```

Fig. 2.2.6 Terminando de configurar con el comando setup.

Y le damos N luego procederemos hacerlo.

Entramos a la manager con la dirección IP 192.168.1.182 en el Navegador introducimos las credenciales de acceso y nos vamos donde dice DEVICE en GLOBAL luego en New.

Ponemos el nombre que le pusimos desde la línea de comandos y la contraseña que va establecer la conexión del sensor con la manager.

Como se ve en la Fig.2.2.7, establecemos la llave compartida en la manager. [8]

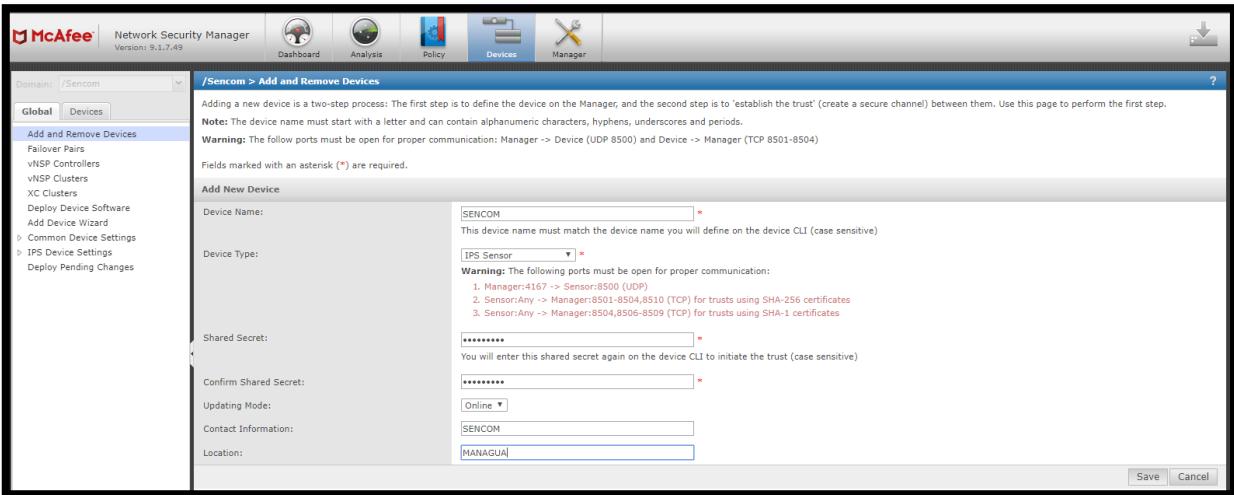


Fig. 2.2.7 Establecer la llave compartida en la manager.

En la Fig. 2.2.8, verificamos la llave compartida en la manager.

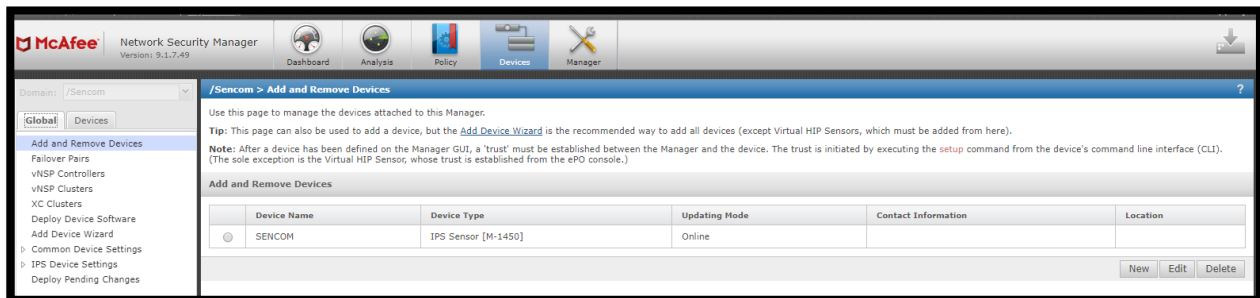


Fig. 2.2.8 Verificación de la llave compartida.

Regresamos al software Putty e introducimos el comando **Shared Secret Key** y con la misma contraseña que habíamos puesto en la manager hacemos ahora desde la línea de comando

En la Fig.2.2.9, presentamos el establecimiento de la llave compartida en el sensor.

```
login as: admin
* * *

Authorized users only. Unauthorized users will be prosecuted
to the full extent of the law.

* * *
admin@_____ 's password:
Access denied
admin@_____ 's password:
Last login: Mon Mar 19 14:02:56 2018 from _____
Trying _____
Connected to _____
Escape character is '\377'.

Hello, this is zebra (version 0.92a).
Copyright 1996-2001 Kunihiro Ishiguro.

intruShell@SENCOM> set sensor sh
intruShell@SENCOM> set sensor sharedsecretkey
```

Fig. 2.2.9 Estableciendo la llave compartida en el sensor.

Ahora para ver que el sensor y la manager tiene la conexión establecida damos el siguiente comando status.

En la Fig. 2.2.10, verificamos la relación entre el sensor y la manager con el comando status en el sensor.

```
[Manager Communications]
Trust Established      : yes (RSA 2048-bit with SHA2 support)
Alert Channel         : up
Log Channel           : up
Authentication Channel : up
Last Error             : None
Alerts Sent            : 35510
Logs Sent              : 11396
```

Fig. 2.2.10 Verificando la relación entre el sensor y la manager.

### 2.3. Actualización del IPS:

En la manager nos vamos donde updating y en Download Device Software, nos muestra todas las actualizaciones para diferentes modelos buscamos nuestro sensor M-1450, seleccionamos la versión 9.1.3.6 y comenzamos el download.

En la Fig. 2.3.1, exhibimos la elección de la versión a actualizar y descargar.

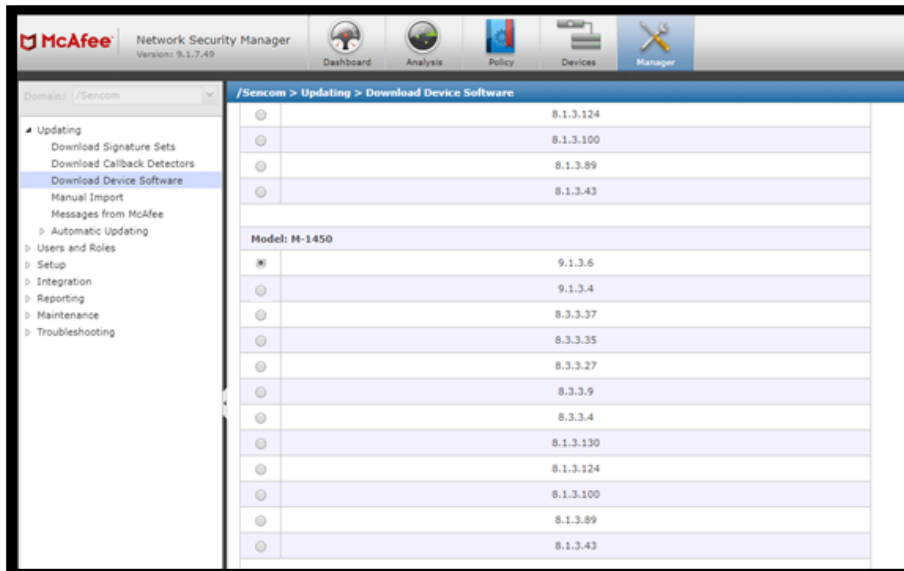


Fig. 2.3.1 Elegir la versión a actualizar y descargar

Ahora nos muestra desde la versión que tenemos y la versión que descargamos ahora damos click en Upgrade.

En la Fig. 2.3.2, presentamos la actualización del IPS.

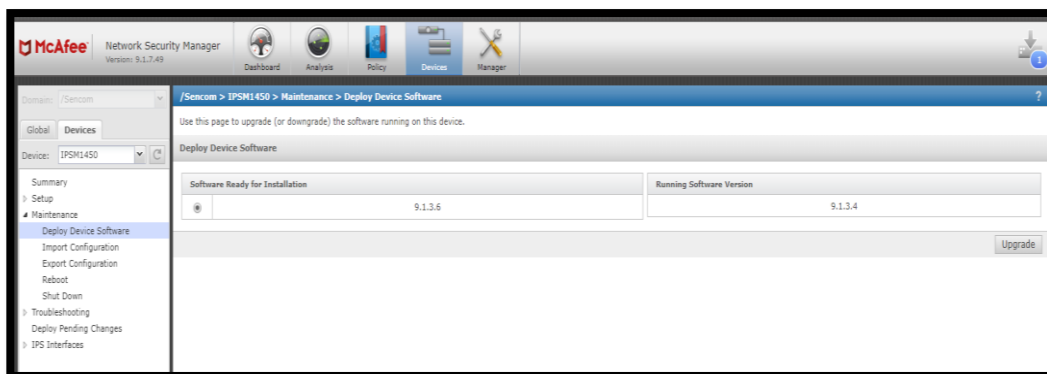
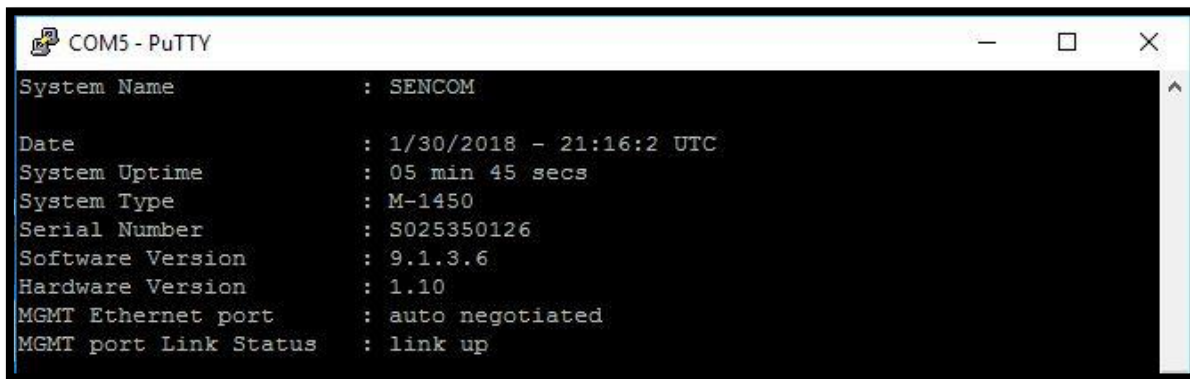


Fig. 2.3.2 Actualizando la versión del IPS del NSP M-1450.

Para comprobar que hemos actualizado a la última versión nos vamos al software Putty para ver la actualización con el comando status.

En la Fig. 2.3.3, mostramos la última versión disponible para el IPS.

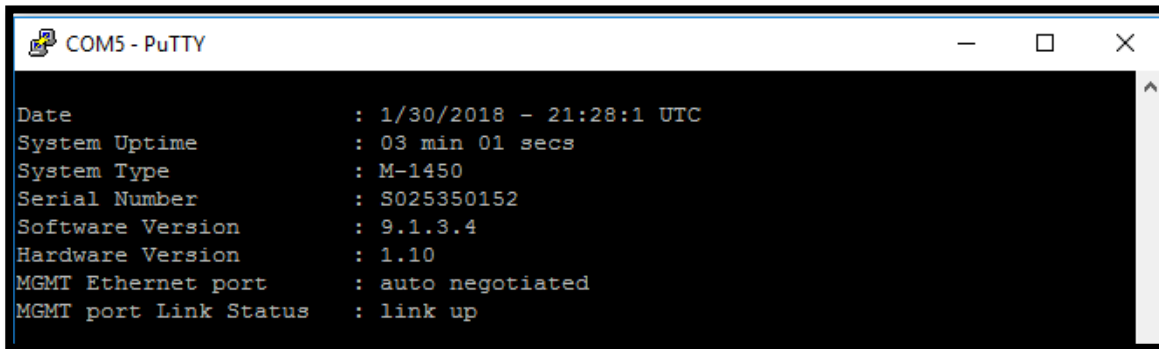


```
COM5 - PuTTY
System Name      : SENCOM
Date             : 1/30/2018 - 21:16:2 UTC
System Uptime    : 05 min 45 secs
System Type      : M-1450
Serial Number     : S025350126
Software Version  : 9.1.3.6
Hardware Version  : 1.10
MGMT Ethernet port : auto negotiated
MGMT port Link Status : link up
```

Fig. 2.3.3 Última versión disponible para el IPS NSP M-1450.

Y la versión que anteriormente es:

En la Fig. 2.3.4, observamos la versión anterior del IPS.



```
COM5 - PuTTY
Date             : 1/30/2018 - 21:28:1 UTC
System Uptime    : 03 min 01 secs
System Type      : M-1450
Serial Number     : S025350152
Software Version  : 9.1.3.4
Hardware Version  : 1.10
MGMT Ethernet port : auto negotiated
MGMT port Link Status : link up
```

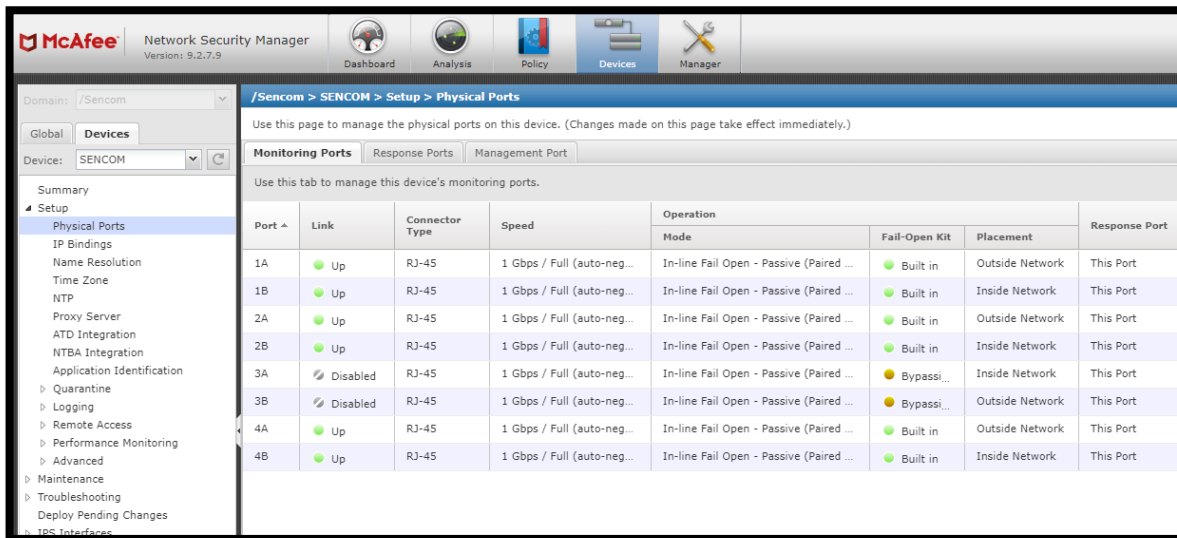
Fig. 2.3.4 Versión anterior del IPS.

Después de tener la conexión con la manager y luego de haber actualizado el IPS procedimos a colocar el sensor en el Rack, para esto tuvimos que hacer cable RJ-45 categoría 6 y medimos la distancia que hay entre el ISP, UTM y el Switch de IP Privada.

Después de colocar los conectores desde la manager estaba en down lo cual lo encendimos y al final mostraremos como un antes y un después de haber implementado este equipo. Esto es en capa 2.



En la Fig. 2.3.5, revelamos la implementación del IPS los enlaces WAN, LAN y AP. En esta parte ya hemos colocado el dispositivo de red en el rack y podemos acceder desde SSH.

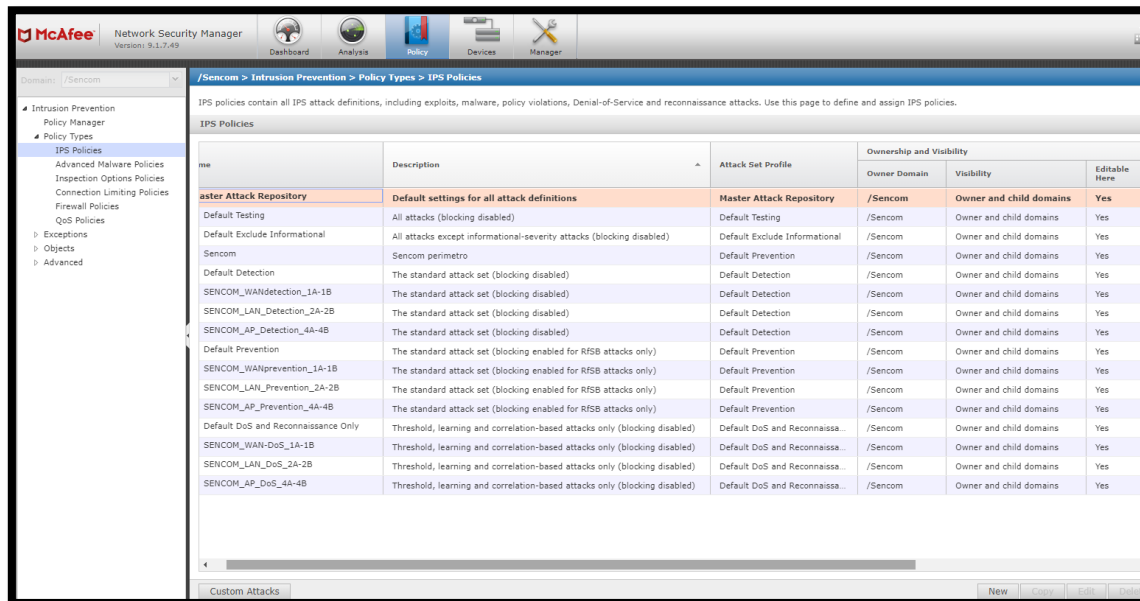


**Fig. 2.3.5 Implementación del IPS con sus enlaces WAN, LAN y AP.**

## 2.4. Políticas del IPS:

Configuramos las políticas del IPS en la manager.

En la Fig.2.4.1, mostramos la configuración de las políticas del IPS.



**Fig. 2.4.1 Configuración de las políticas del IPS.**



**McAfee**

**Network Security Manager**  
Version: 5.5.7.43

Dashboard

Analysis

Policy

Devices

Manager

Domain: /Sencoms

Intrusion Prevention

Policy Manager

Policy Types

IPS Policies

Advanced Malware Policies

Inspection Options Policies

Connection Linking Policies

Firewall Policies

QoS Policies

Exceptions

Objects

Advanced

/Sencoms > Intrusion Prevention > Policy Types > IPS Policies

7

IPS policies contain all IPS attack definitions, including exploits, malware, policy violations, Denial-of-Service and reconnaissance attacks. Use this page to define and assign IPS policies.

IPS Policies

	Attack Set Profile	Ownership and Visibility			Last Updated			By	Assignments
		Owner Domain	Visibility	Editable Here	Active Revision	Time			
Definitions	Master Attack Repository	/Sencoms	Owner and child domains	Yes	1	Feb 28, 2018 01:04:11		admin	n/a
Severity attacks (blocking disabled)	Default Testing	/Sencoms	Owner and child domains	Yes	1	Feb 28, 2018 01:04:12		admin	0
	Default Exclude (Informational)	/Sencoms	Owner and child domains	Yes	1	Feb 28, 2018 01:04:12		admin	0
	Default Prevention	/Sencoms	Owner and child domains	Yes	2	Feb 28, 2018 01:04:13		admin	0
ig disabled)	Default Detection	/Sencoms	Owner and child domains	Yes	1	Feb 28, 2018 01:04:11		admin	0
ig disabled)	Default Detection	/Sencoms	Owner and child domains	Yes	3	Mar 02, 2018 15:03:36		admin	0
ig disabled)	Default Detection	/Sencoms	Owner and child domains	Yes	1	Mar 02, 2018 15:35:07		admin	0
ig disabled)	Default Detection	/Sencoms	Owner and child domains	Yes	1	Mar 02, 2018 15:35:57		admin	0
ig enabled for RFB attacks only)	Default Prevention	/Sencoms	Owner and child domains	Yes	2	Feb 28, 2018 01:04:13		admin	0
ig enabled for RFB attacks only)	Default Prevention	/Sencoms	Owner and child domains	Yes	1	Mar 02, 2018 15:04:38		admin	1
ig enabled for RFB attacks only)	Default Prevention	/Sencoms	Owner and child domains	Yes	1	Mar 02, 2018 15:37:15		admin	1
ig enabled for RFB attacks only)	Default Prevention	/Sencoms	Owner and child domains	Yes	1	Mar 02, 2018 15:40:59		admin	1
ion-based attacks only (blocking disabled)	Default DoS and Reconnaissance	/Sencoms	Owner and child domains	Yes	1	Feb 28, 2018 01:04:12		admin	0
ion-based attacks only (blocking disabled)	Default DoS and Reconnaissance	/Sencoms	Owner and child domains	Yes	1	Mar 02, 2018 15:06:39		admin	0
ion-based attacks only (blocking disabled)	Default DoS and Reconnaissance	/Sencoms	Owner and child domains	Yes	1	Mar 02, 2018 15:38:03		admin	0
ion-based attacks only (blocking disabled)	Default DoS and Reconnaissance	/Sencoms	Owner and child domains	Yes	1	Mar 02, 2018 15:43:51		admin	0

Custom Attacks

New | Cancel | Edit | Delete

**Fig. 2.4.3 Guardando las políticas del IPS.**

En la Fig.2.4.4, presentamos las políticas de Firewall para denegar el tráfico proveniente de Rusia y China.

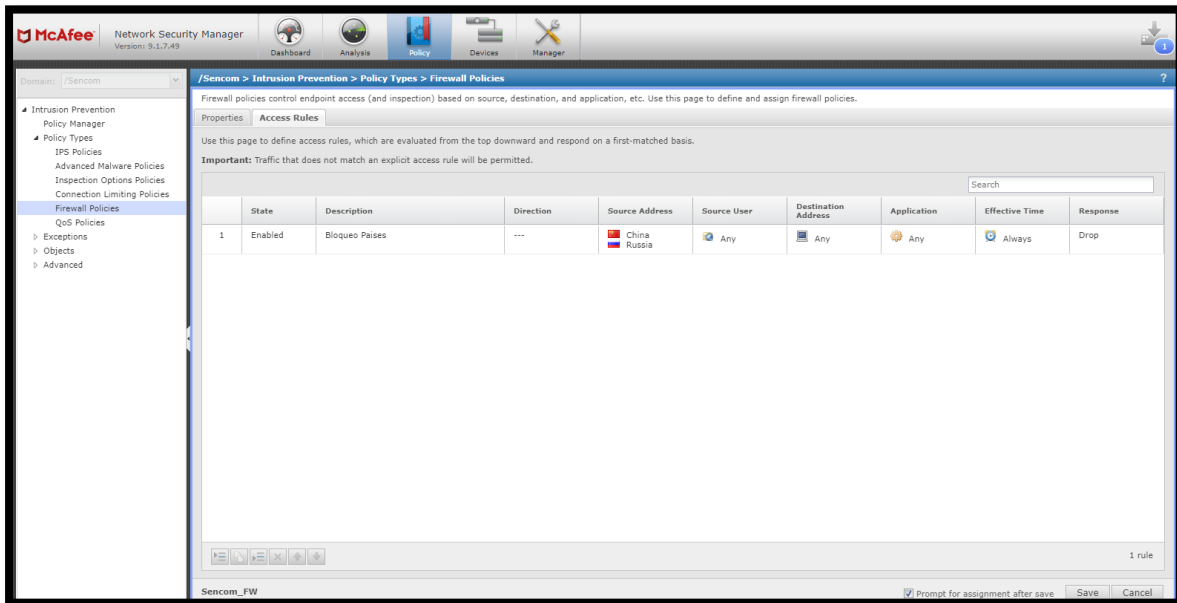


Fig. 2.4.4 Políticas de Firewall del IPS.

En la Fig. 2.4.5, enseñamos como estaba la red de computadoras antes de la implementación del IPS.

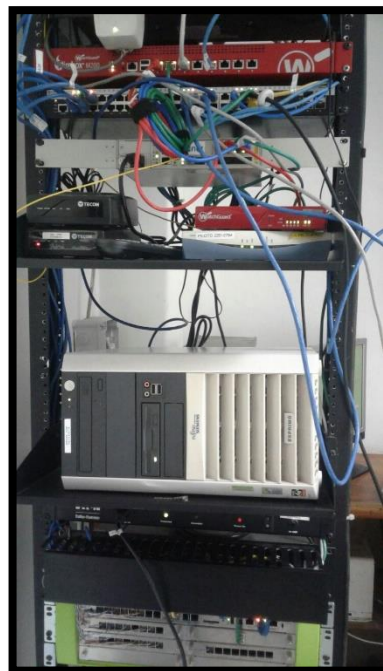


Fig. 2.4.5 Antes de implementar el IPS.

En la Fig. 2.4.6, mostramos después de implementar el IPS nos quedó de la siguiente manera:

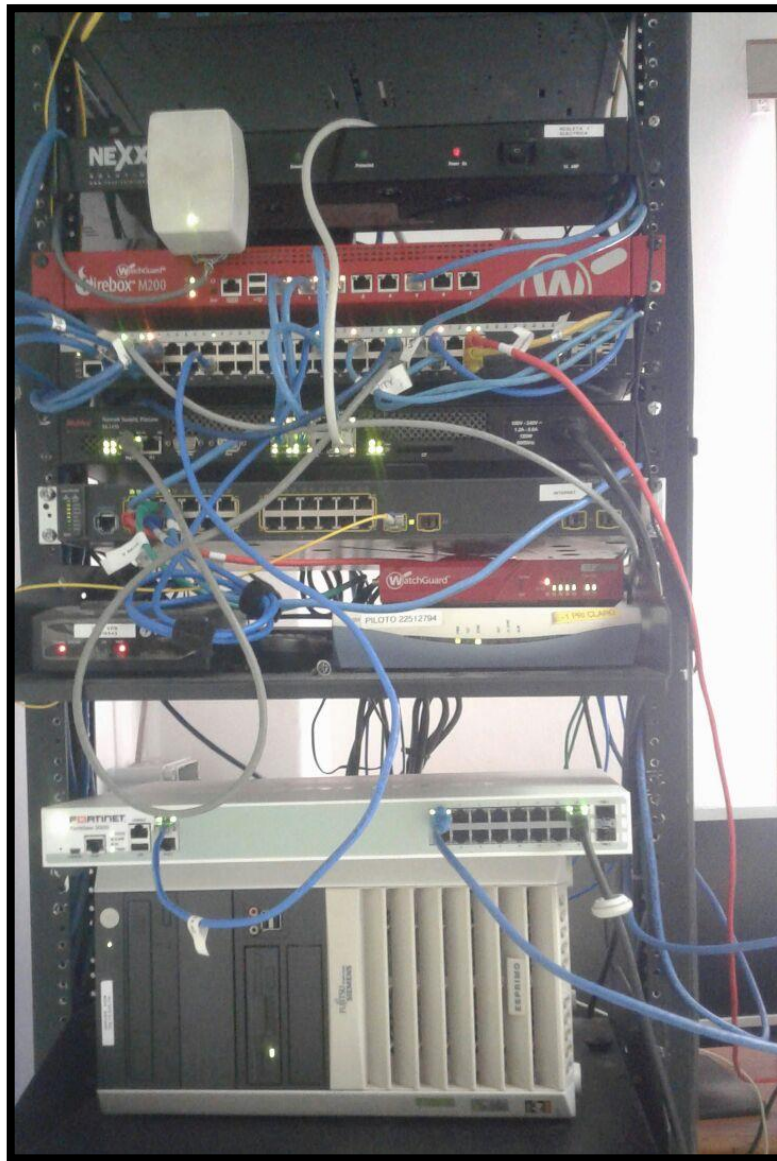


Fig. 2.4.6 Después de implementar el IPS.

## Capítulo 3

### 3. Servidor DNS:

#### 3.1. Teoría:

Proviene de las palabras (Domain Name System o Sistema de nombres de dominio) su función es que traduce nombres de dominio a IPs y viceversa. En las redes TCP/IP cada dispositivos final dispone de una dirección IP para la comunicación con el resto de PCs es como decir que es un identificador único que lo diferencia del resto de dispositivos. Durante el proceso de búsqueda de un nombre, funcionan como clientes DNS, Consultando otros servidores para resolver completamente el nombre buscado. Un diagrama jerárquico de cómo funciona un servidor DNS.

En la Fig. 3.1.1, exhibimos los tipos de jerarquía para un servidor DNS.

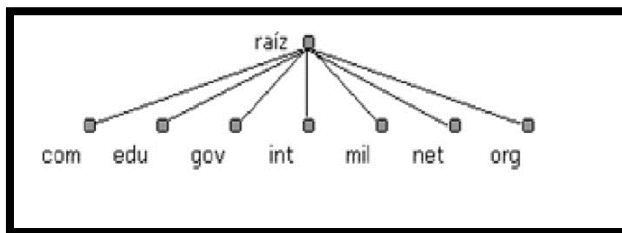


Fig. 3.1.1 Tipos de jerarquía para un servidor DNS.

Los Forwarders son los encargados de reenviar a los otros DNS internos para reenviar consultas y resolver nombres de dominios externos o fuera del sitio.

En la Fig. 3.1.2, indicamos el funcionamiento del Forwarders.

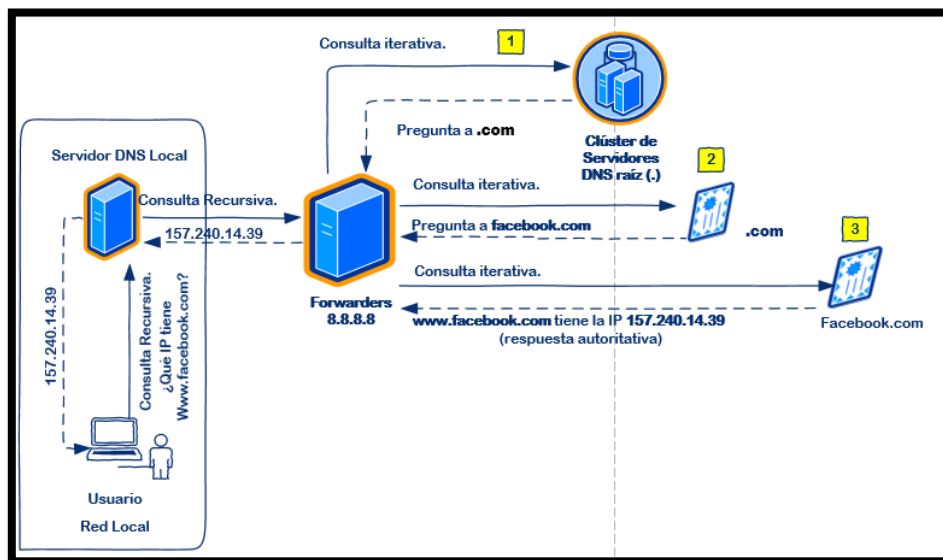


Fig. 3.1.2 Funcionamiento del Forwarders.

### 3.2. Implementación:

Después de preparar una máquina virtual en nuestro segmento de IP Privada con todas las características básicas en hardware y ya con el sistema operativo LINUX listo, Iniciamos la instalación. [18]

En la Fig. 3.2.1, evidenciamos la selección del idioma en la instalación del servidor DNS.

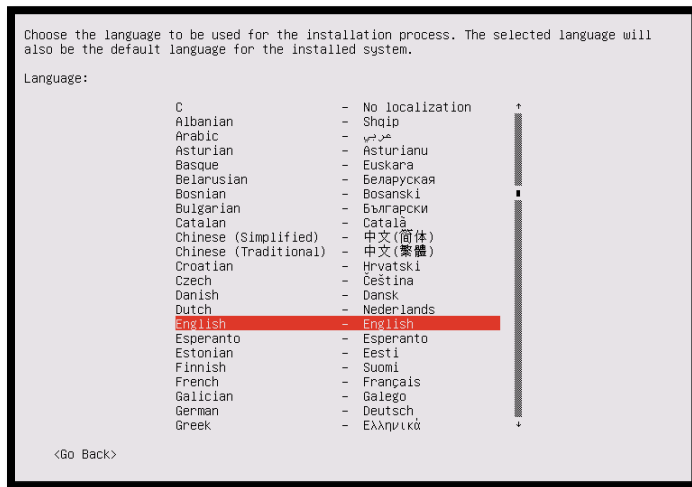


Fig. 3.2.1 Selección del idioma de instalación en Linux.

En la Fig. 3.2.2, señalamos la elección del tipo de teclado en el servidor.

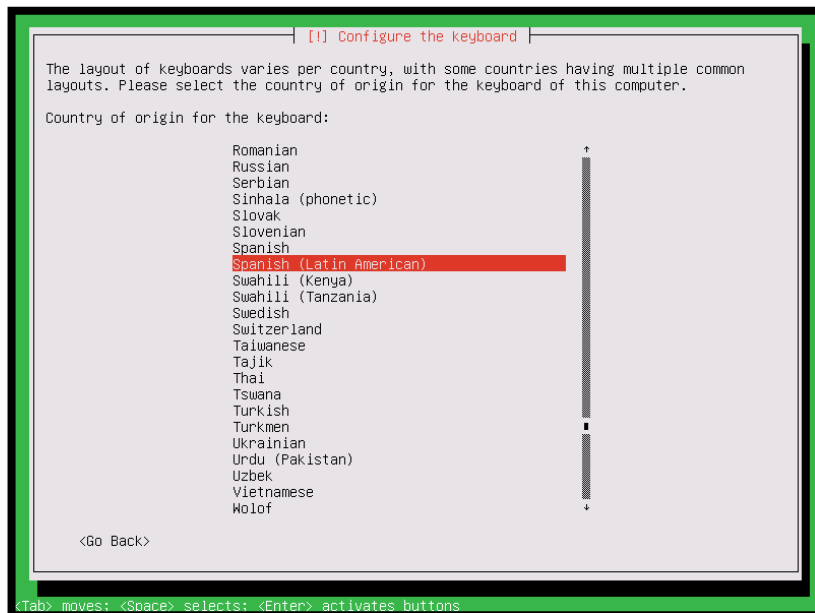
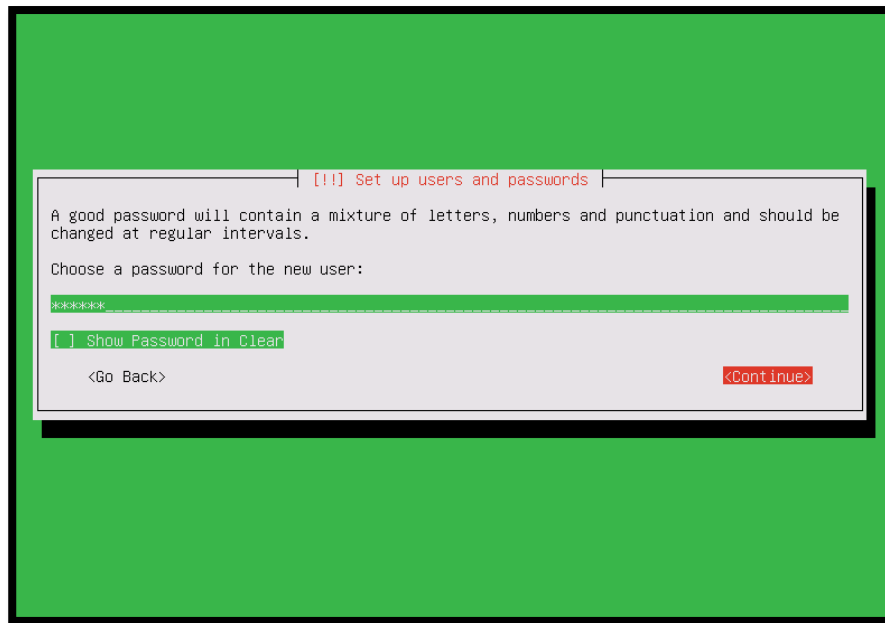


Fig. 3.2.2 Elección del tipo de teclado en el servidor

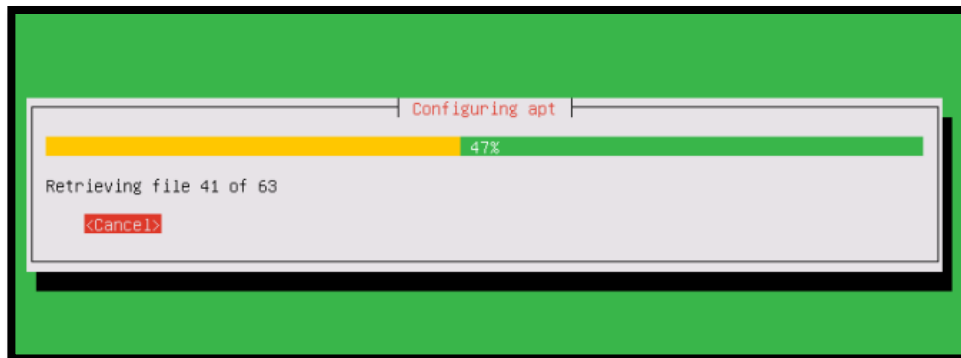
En el proceso de instalación del sistema operativo es necesario establecer el idioma en nuestro caso es en inglés y el tipo de teclado por los diferentes caracteres que son necesarios para programar.

En la Fig. 3.2.3, indicamos el establecimiento de las credenciales de acceso.



**Fig. 3.2.3 Establecer las Credenciales de acceso.**

En la Fig. 3.2.4, mostramos la instalación del sistema del servidor DNS.



**Fig. 3.2.4 Instalación del Sistema Operativo.**

En la Fig. 3.2.5, presentamos el ingreso de nuestras credenciales para después acceder a la plataforma del Zentyal. Esperamos que termine de configurar. [12]

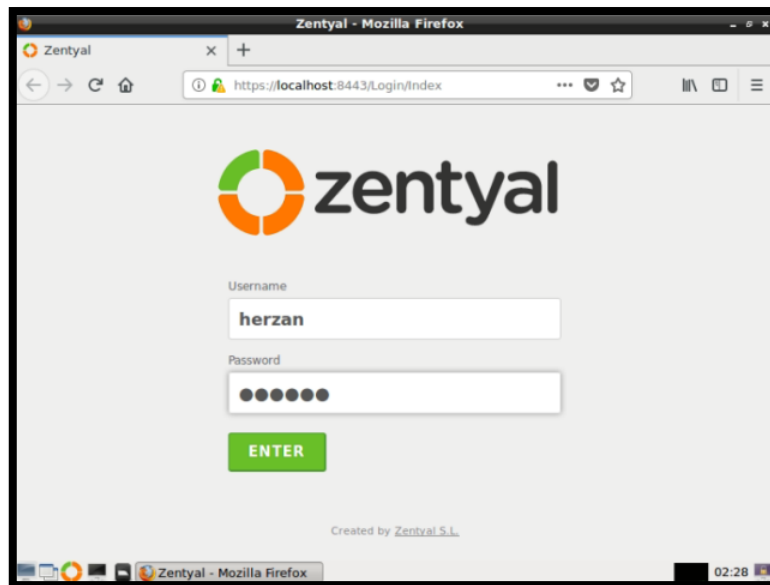


Fig. 3.2.5 Ingreso de las Credenciales.

Luego posteriormente descargamos archivos necesarios para la ejecución de nuestro Server procedimos a configurar nuestro servidor DNS.

En la Fig. 3.2.6, observamos la elección de los módulos a instalar en el Server.

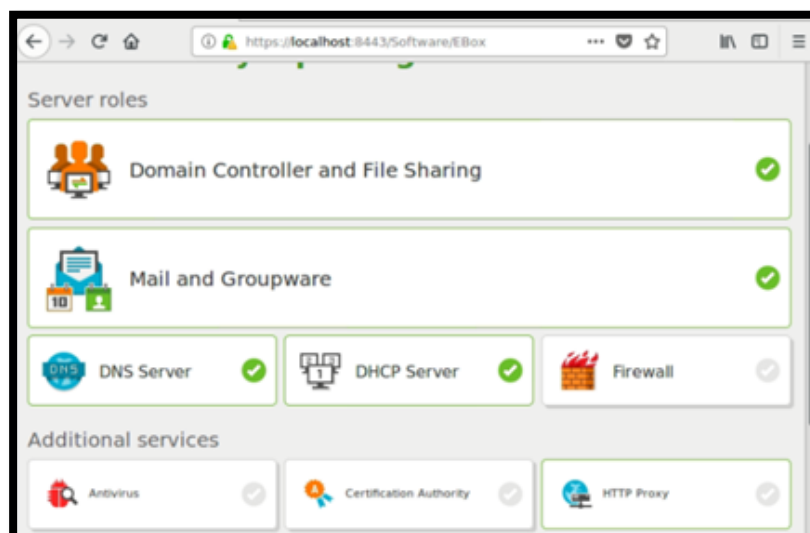


Fig. 3.2.6 Elección de los módulos a instalar.



Al momento de seleccionar los módulos necesarios para nuestro servidor DNS va a instalar los paquetes en nuestra plataforma y en el servidor. De este modo podamos configurarlo.

En la Fig. 3.2.7, enseñamos la descarga e instalación de los paquetes requeridos.

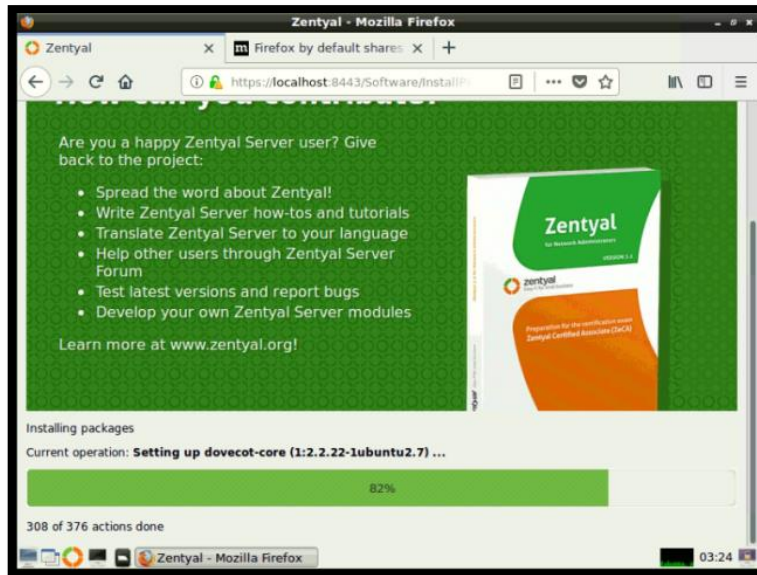


Fig. 3.2.7 Descarga e Instalación de los paquetes requeridos.

En la Fig. 3.2.8, exponemos la configuración de la interfaz externa.



Fig. 3.2.8 Configuración de la interfaz Externa.

Establecemos el nombre del dominio por el cual nuestro servidor DNS estará traduciendo los diferentes sitios Web por nombres. Esperamos que se guarden los cambios hechos para acceder a la plataforma del Zentyal.

En la Fig. 3.2.9, revelamos los ajustes del Nombre de Dominio.

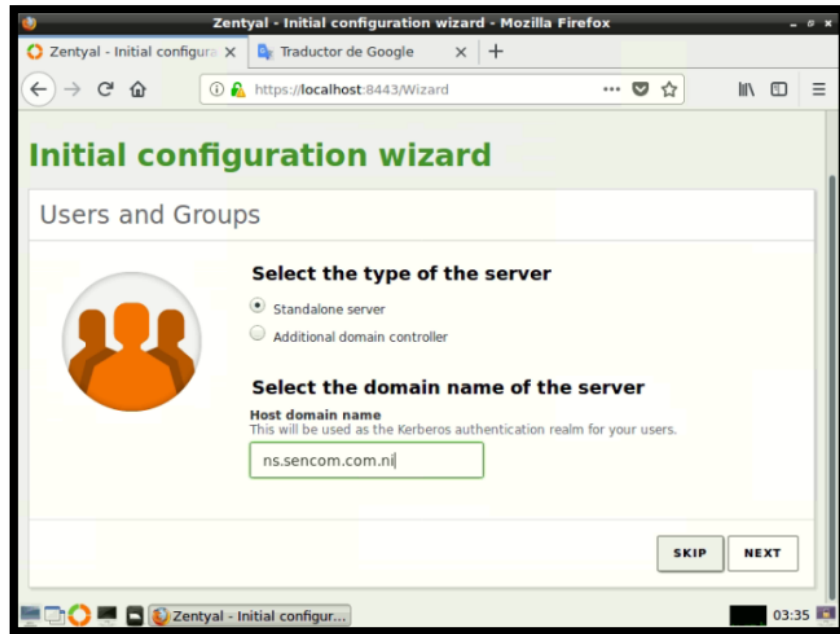


Fig. 3.2.9 Ajuste del Nombre de Dominio.

En la Fig. 3.2.10, observamos la configuración realizada.

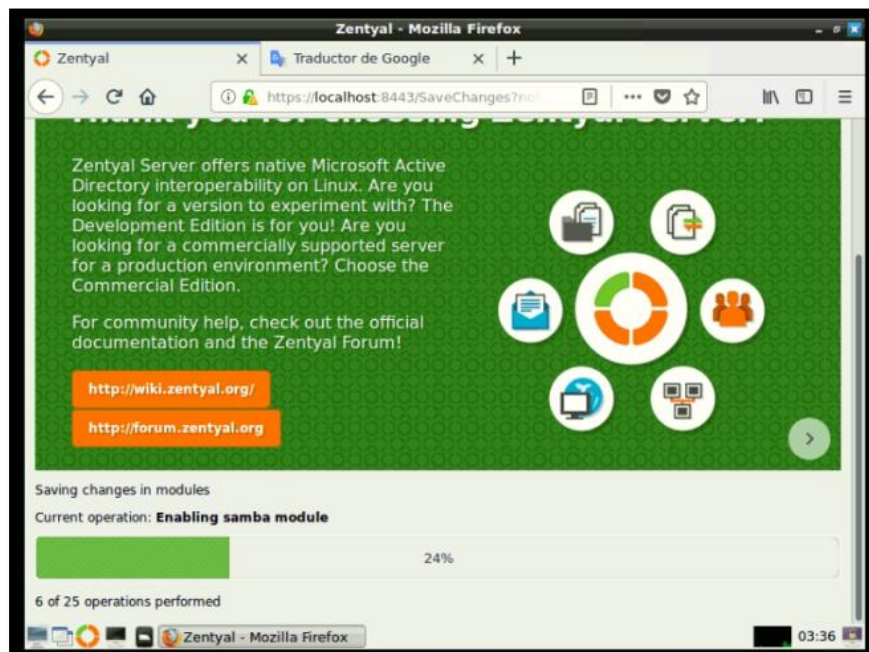


Fig. 3.2.10 Estableciendo las configuraciones realizadas.

Asignamos nuestro direccionamiento de IP Privado en la plataforma como cualquier servidor es necesario que sea Estático y guardamos los cambios.

En la siguiente Fig. 3.2.11, enseñamos la configuración de la dirección IP del server.

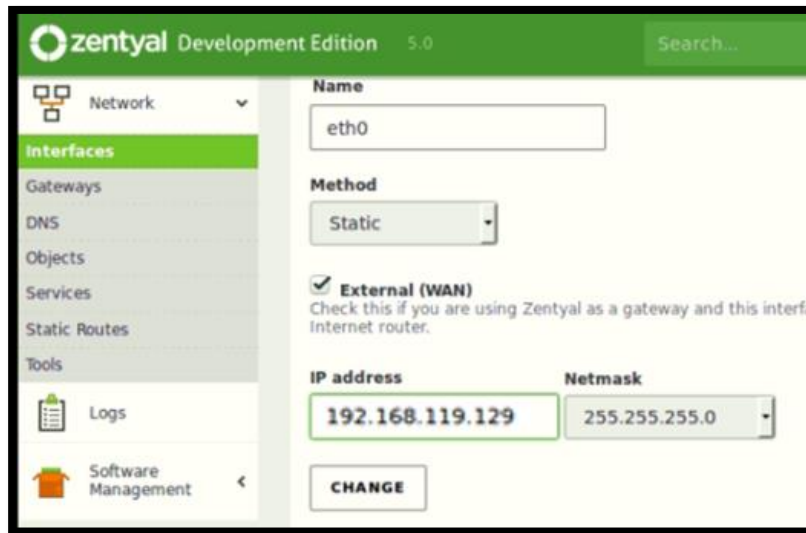


Fig. 3.2.11 Configurando la Dirección IP del Server.

En la Fig. 3.2.12, guardamos los cambios hechos en el server.

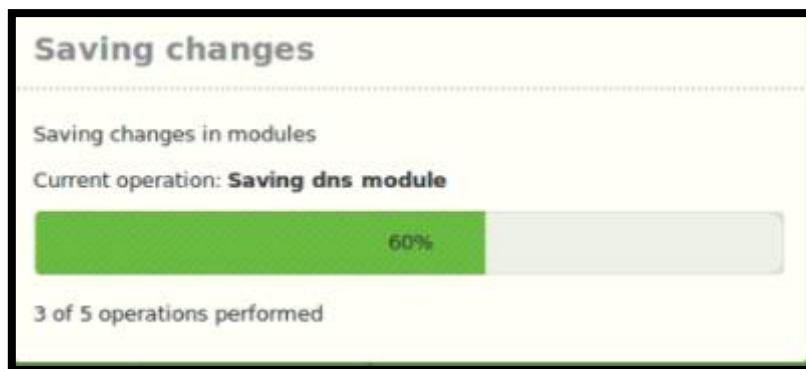


Fig. 3.2.12 Guardando los Cambios Realizados.

En la Fig. 3.2.13, verificamos los módulos activados en el servidor DNS.

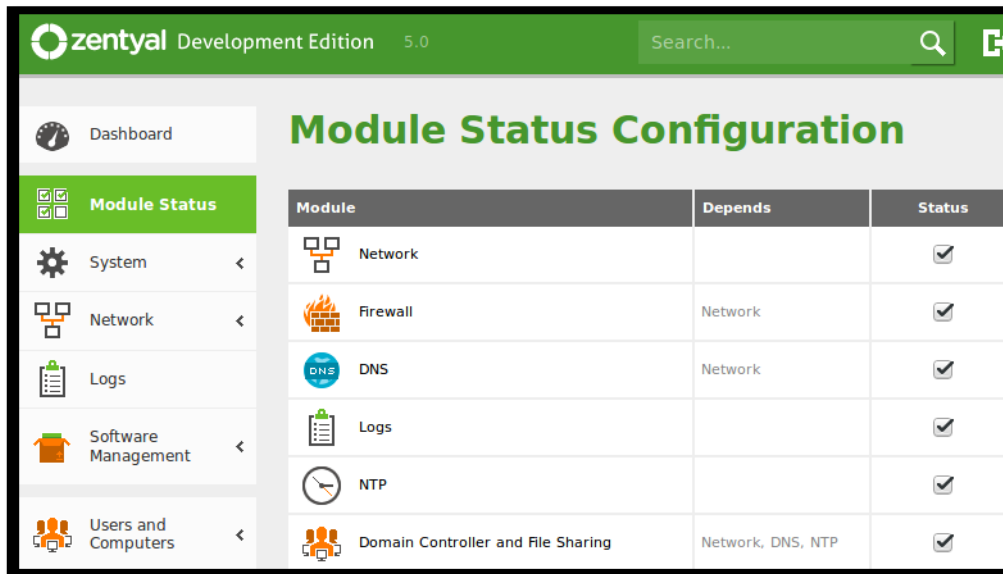


Fig. 3.2.13 Verificación de los módulos activados en el server.

En la Fig. 3.2.14, podemos observar la habilitación de la cache del DNS transparente.

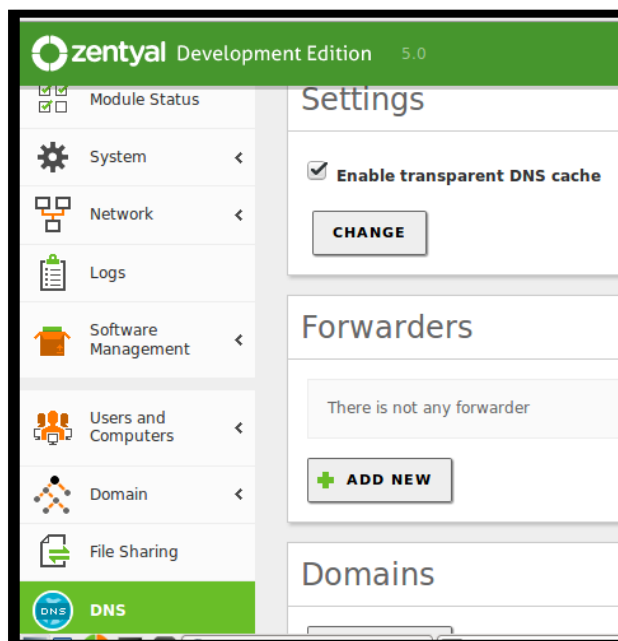


Fig. 3.2.14 Habilidad de la cache del DNS transparente.

En nuestro servidor DNS para que resuelva los nombres de los sitios Web con sus debidos servidores es necesario tener los reenviadores o Forwarders en nuestro caso añadimos a google.

Como se ve en la Fig. 3.2.15, añadimos los Forwarders de los DNS de Google.

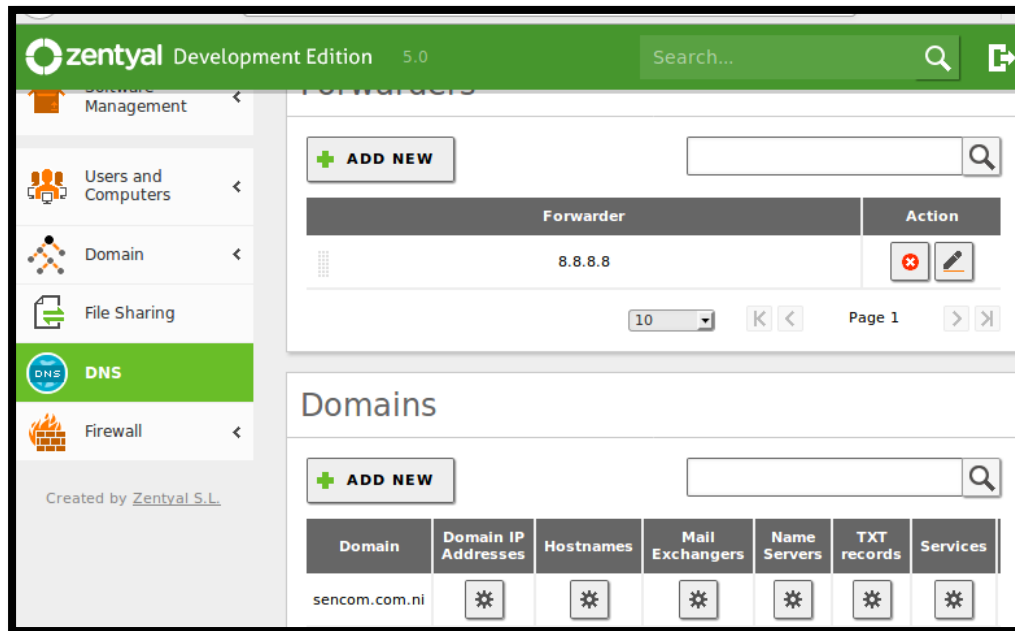


Fig. 3.2.15 Añadir los Forwarders de los DNS de Google.

En la Fig. 3.2.16, presentamos la configuración de nuestro dominio lo cual añadimos nuestra dirección IP fija del Servidor y también nuestro Gateway.

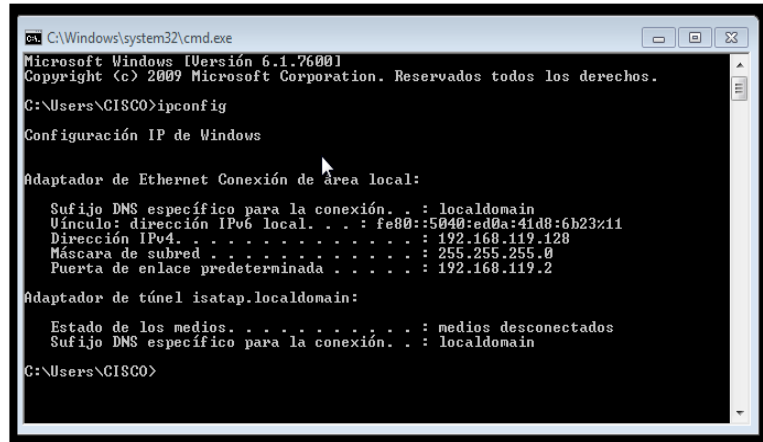


Fig. 3.2.16 Configuración de nuestro dominio.

### 3.3. Prueba del Servidor DNS:

Ahora con el comando nslookup en una máquina virtual Windows 7 del mismo rango de red nos dispondremos a verificar si el Servidor DNS está funcionando debidamente.

En la Fig. 3.3.1, comprobamos nuestra dirección IP en la PC con el comando ipconfig desde el cmd.



```
C:\Windows\system32\cmd.exe
Microsoft Windows [Versión 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. Reservados todos los derechos.

C:\Users\CISCO>ipconfig

Configuración IP de Windows

Adaptador de Ethernet Conexión de área local:

    Sufijo DNS específico para la conexión. . . : localdomain
    Vínculo: dirección IPv6 local. . . . . : fe80::5040:ed0a:41d8:6b23%11
    Dirección IPv4. . . . . : 192.168.119.128
    Máscara de subred . . . . . : 255.255.255.0
    Puerta de enlace predeterminada . . . . . : 192.168.119.2

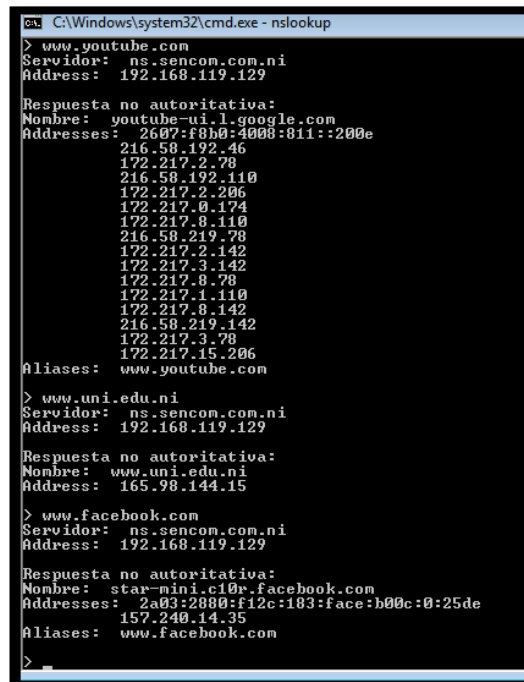
Adaptador de túnel isatap.localdomain:

    Estado de los medios. . . . . : medios desconectados
    Sufijo DNS específico para la conexión. . : localdomain

C:\Users\CISCO>
```

Fig. 3.3.1 Comprobando nuestra dirección IP en la PC.

Como se ve en la Fig. 3.3.2, verificamos el servidor DNS.



```
C:\Windows\system32\cmd.exe - nslookup

> www.youtube.com
Servidor: ns.sencom.com.ni
Address: 192.168.119.129

Respuesta no autoritativa:
Nombre: youtube-ui.l.google.com
Addresses: 2607:f8b0:4008:811::200e
216.58.192.46
172.217.2.78
216.58.192.110
172.217.2.206
172.217.0.174
172.217.8.110
216.58.219.78
172.217.2.142
172.217.3.142
172.217.8.78
172.217.1.110
172.217.8.142
216.58.219.142
172.217.3.78
172.217.15.206
Aliases: www.youtube.com

> www.uni.edu.ni
Servidor: ns.sencom.com.ni
Address: 192.168.119.129

Respuesta no autoritativa:
Nombre: www.uni.edu.ni
Address: 165.98.144.15

> www.facebook.com
Servidor: ns.sencom.com.ni
Address: 192.168.119.129

Respuesta no autoritativa:
Nombre: star-mini.c10r.facebook.com
Addresses: 2a03:2880:f12c:183:face:b00c:0:25de
157.240.14.35
Aliases: www.facebook.com

>
```

Fig. 3.3.2 Verificación del servidor DNS.

## Capítulo 4

### 4. Fortimail:

Consiste en un Antispam y servidor de correo. El usuario recibe un mensaje por cierta persona pero en el contenido del mensaje es enviado un enlace a otro sitio vulnerable y eso se conoce como phishing.

**Antispam:** Es un método para no recibir correo basura, tanto para los usuarios finales como para los administradores de los sistemas de correos electrónicos usan diferentes técnicas contra ellos. Estas técnicas han sido incorporadas en distintos productos, servicios y software para aliviar la carga que cae sobre usuarios y administradores. No hay una forma perfecta para solucionar este problema de Spam, entre las múltiples unas funcionan mejor que otras, rechazando así en su totalidad y en algunos casos el correo deseado para eliminar completamente el Spam.

**Detección de spam:** Consiste en perder gran cantidad de correos electrónicos basura para reducir la cantidad de correos legítimos. Se basa en el contenido del mensaje del correo electrónico, ya sea por la detección de palabras clave como (Viagra) o por medios estadísticos. Los métodos antes mencionado pueden ser muy precisos cuando se sintoniza con los correos legítimos que la persona recibe, se puede cometer errores tales como el envío de contenido destinados a una dirección particular o más bien a una distribución masiva.

Existen sitios conocidos como listas negras, estos son direcciones IP de Spammers conocido, también están los spamtraps son direcciones de correo electrónico invalidas que no se utilizan durante mucho tiempo para recoger correos basura.

#### 4.1. Implementación:

### ARQUITECTURA.

La arquitectura de la solución es bastante sencilla al implementar el Fortimail, en la cual tenemos una sola conexión (En este caso es Virtual). la arquitectura quedara asi:

En la Fig. 4.1.1, observamos la arquitectura de implementación del Fortimail en SENCOM.

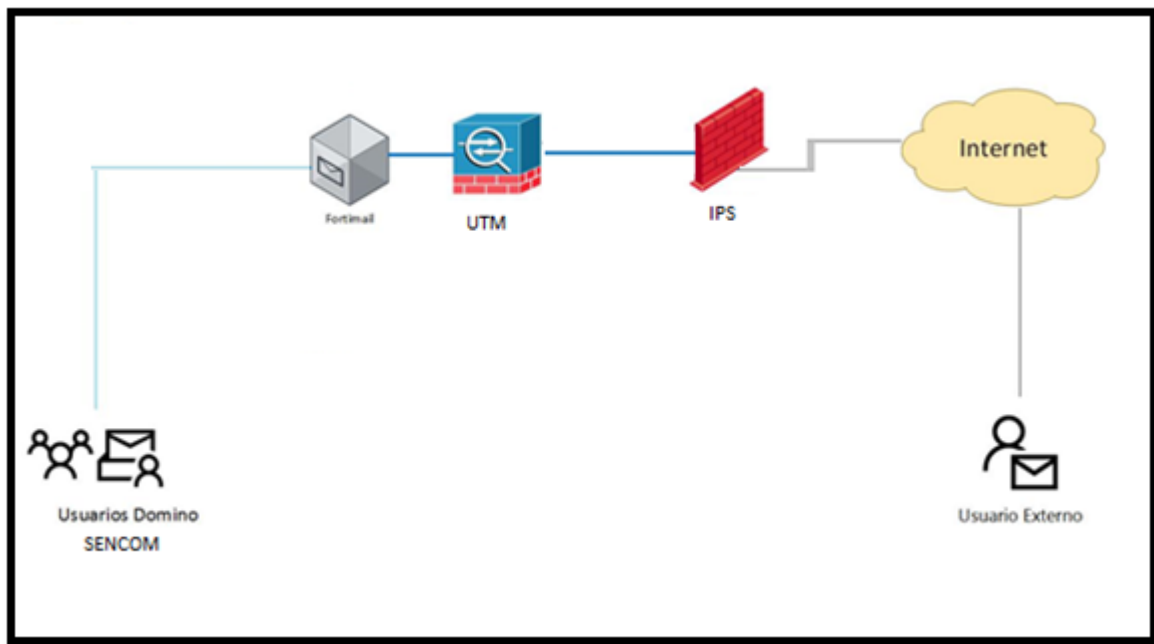


Fig. 4.1.1 Arquitectura de implementación del Fortimail.



## 4.2. Instalación del Fortimail.

El Fortimail al ser una maquina virtual se instalara sobre la plataforma VmWare, lo que se usa para instalar es una plantilla OVF que se descarga desde la pagina web de Fortinet con una cuenta previamente creada:

Primero accedemos al sitio:

<https://support.fortinet.com/Download/FirmwareImages.aspx> nos logueamos con el usuario y nos dara una pagina como esta, donde damos clic en “Download → Firmware Images”: [6]

En la Fig. 4.2.1, enseñamos como se descarga el Firmware desde la pagina oficial de Fortinet.

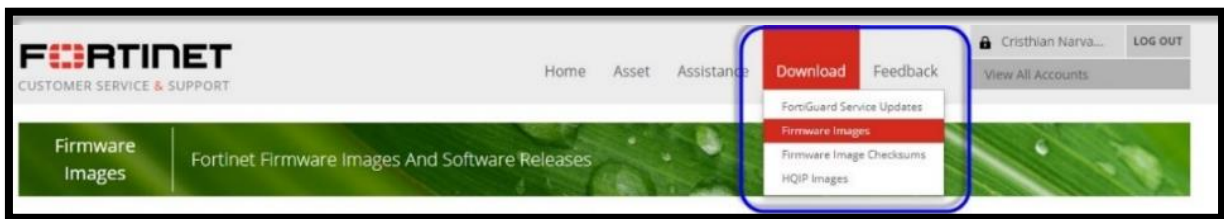


Fig. 4.2.1 Descarga del Firmware desde la página oficial de Fortinet.

En la siguiente Fig. 4.2.2, mostramos la selección del producto el cual implementaremos en nuestro caso es el Fortimail:

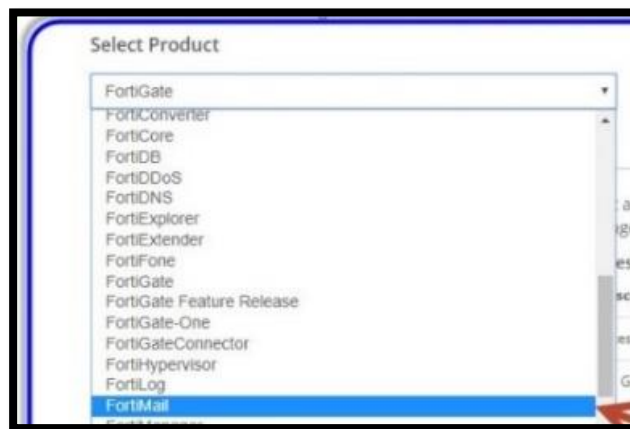


Fig. 4.2.2 Selección del producto el cual implementaremos.

Luego de que hayamos seleccionado la ultima version disponible del Fortimail como se ve en la Fig. 4.2.3.

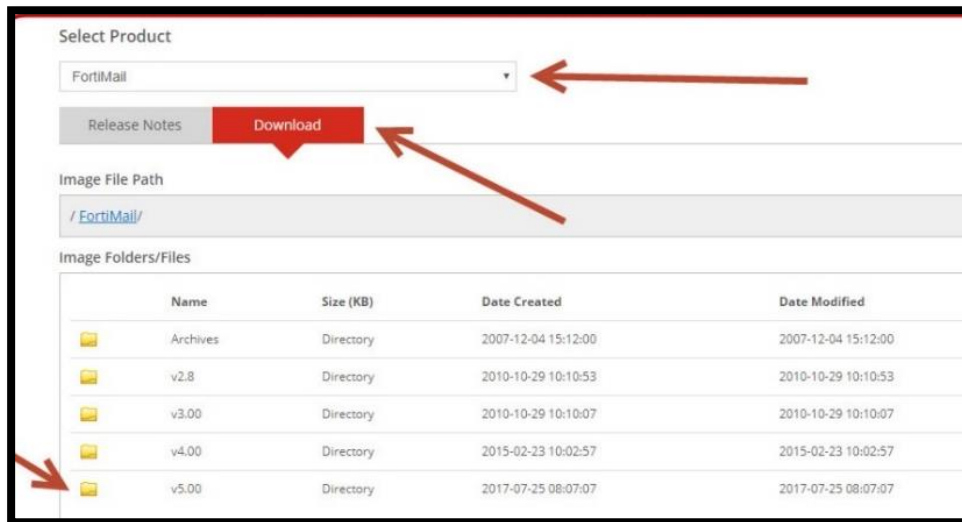


Fig. 4.2.3 Elección de la última versión disponible del Fortimail.

En la siguiente Fig. 4.2.4, enseñamos el procedimiento para descargar la ultima version disponible del Firmware, esa es la imagen que vamos a descargar via HTTPS:

The screenshot shows a list of files in a table. The last row, 'FML\_VM-64-v54-build0692-FORTINET.out.ovf.zip', is highlighted with a red box and a red arrow pointing to its 'HTTPS Checksum' link.

Name	Size (KB)	Date Created	Date Modified	HTTPS Checksum
FML_3000E-64-v54-build0692-FORTINET.out	93,642	2017-07-25 09:07:47	2017-07-25 09:07:47	<a href="#">HTTPS Checksum</a>
FML_3200E-64-v54-build0692-FORTINET.out	93,619	2017-07-25 09:07:28	2017-07-25 09:07:28	<a href="#">HTTPS Checksum</a>
FML_400E-v54-build0692-FORTINET.out	93,493	2017-07-25 09:07:41	2017-07-25 09:07:41	<a href="#">HTTPS Checksum</a>
FML_60D-v54-build0692-FORTINET.out	92,413	2017-07-25 09:07:02	2017-07-25 09:07:02	<a href="#">HTTPS Checksum</a>
FML_VM-64-v54-build0692-FORTINET.out	92,855	2017-07-25 09:07:06	2017-07-25 09:07:06	<a href="#">HTTPS Checksum</a>
FML_VM-64-v54-build0692-FORTINET.out.ovf.zip	178,856	2017-07-25 09:07:49	2017-07-25 09:07:49	<a href="#">HTTPS Checksum</a>

Fig. 4.2.4 Procediendo a descargar la última versión disponible del firmware.

En la Fig. 4.2.5, observamos como se descargara el archivo en formato Rar de esta forma:


Nombre	Fecha de modifica...	Tipo	Tamaño
 FML_VM-64-v53-build0634-FORTINET.out.ovf.zip	25/05/2017 08:40 a...	Archivo WinRAR Z...	153,838 KB

Fig. 4.2.5 Descargando la versión 5.4 del Fortimail.

Lo decomprimos y veremos varios OVF y otros archivos que son parte de esos OVF, lo que los diferencian es el tamaño en disco que la plantilla tiene configurado en este caso seria la de **250 Gb.** [7]

Como se ve en la Fig. 4.2.6, seleccionamos el archivo a desplegar en nuestro Hypervisor.

















Nombre	Fecha de modifica...	Tipo	Tamaño
 FML_VM-64-v53-build0634-FORTINET.out.ovf.zip	25/05/2017 08:40 a...	Archivo WinRAR Z...	153,838 KB
 fortimail-vm-64bit-250gb-hw7.ovf	28/02/2017 07:50 ...	Open Virtualizatio...	61 KB
 fortimail-vm-64bit-1024gb-hw7.ovf	28/02/2017 07:50 ...	Open Virtualizatio...	61 KB
 fortimail-vm-64bit-2048gb-hw7.ovf	28/02/2017 07:50 ...	Open Virtualizatio...	61 KB
 fortimail-vm-64bit-4096gb-hw7.ovf	28/02/2017 07:50 ...	Open Virtualizatio...	61 KB
 fortimail-vm-64bit-8192gb-hw7.ovf	28/02/2017 07:50 ...	Open Virtualizatio...	61 KB
 fortimail-vm-64bit-12288gb-hw7.ovf	28/02/2017 07:50 ...	Open Virtualizatio...	61 KB
 fortimail-vm-64bit-24576gb-hw7.ovf	28/02/2017 07:50 ...	Open Virtualizatio...	61 KB
 fortimail-vm-disk1.vmdk	28/02/2017 07:50 ...	VMware virtual dis...	154,818 KB
 fortimail-vm-disk2-250gb.vmdk	28/02/2017 07:50 ...	VMware virtual dis...	117 KB
 fortimail-vm-disk2-1024gb.vmdk	28/02/2017 07:50 ...	VMware virtual dis...	244 KB
 fortimail-vm-disk2-2048gb.vmdk	28/02/2017 07:50 ...	VMware virtual dis...	372 KB
 fortimail-vm-disk2-4096gb.vmdk	28/02/2017 07:50 ...	VMware virtual dis...	628 KB
 fortimail-vm-disk2-8192gb.vmdk	28/02/2017 07:50 ...	VMware virtual dis...	1,183 KB
 fortimail-vm-disk2-12288gb.vmdk	28/02/2017 07:50 ...	VMware virtual dis...	1,678 KB
 fortimail-vm-disk2-24576gb.vmdk	28/02/2017 07:50 ...	VMware virtual dis...	3,288 KB

Fig. 4.2.6 Selección del archivo a desplegar en nuestro Hypervisor

En la Fig. 4.2.7, presentamos el despliegue del OVF del Fortimail para su debida instalacion en el servidor ESXI para poder instalar la imagen, esta es un OVF asi que solo seguimos la ruta: **File → Deploy OVF Template**.

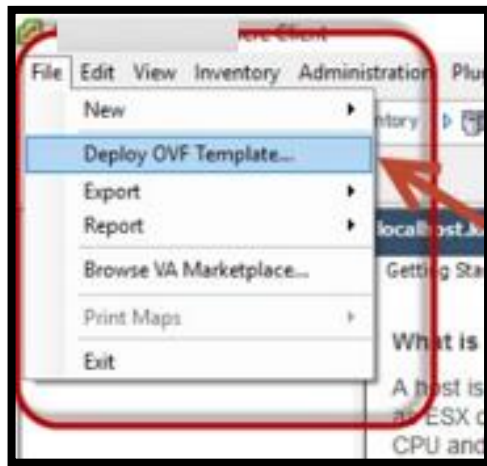


Fig. 4.2.7 Despliegue del OVF del Fortimail para su debida instalación.

Como se ve en la Fig. 4.2.8, seleccionamos el Firmware para el despliegue del Fortimail.

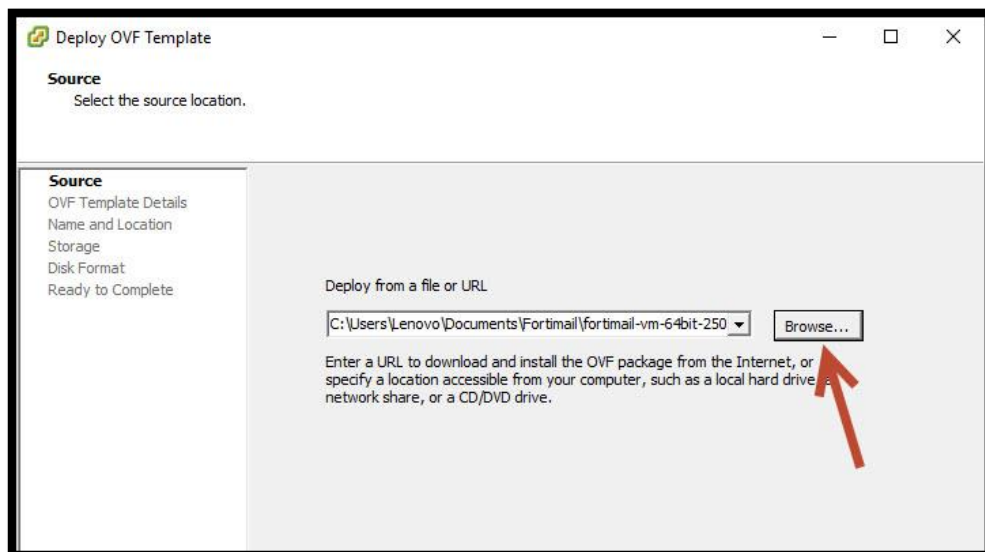


Fig. 4.2.8 Selección del Firmware para el despliegue del Fortimail.

En la Fig. 4.2.9, exponemos la eleccion del archivo necesario del Fortimail.

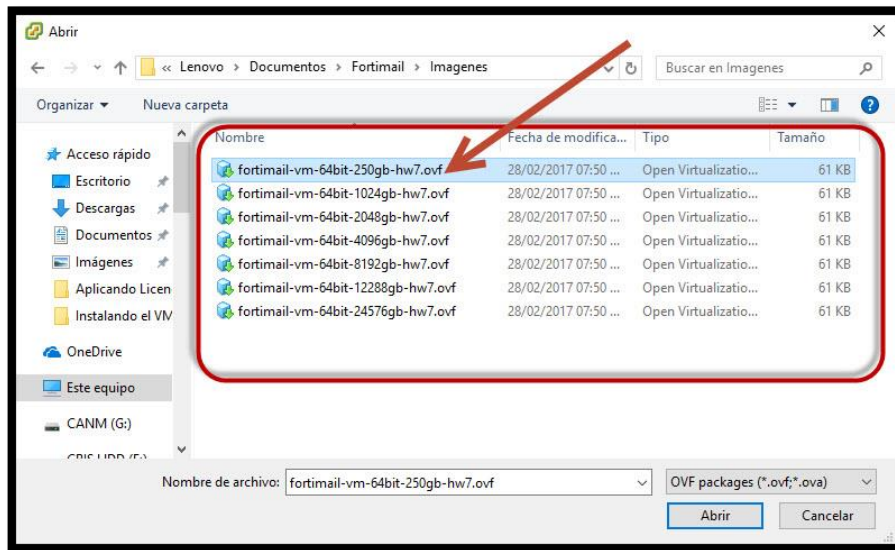


Fig. 4.2.9 Elección del archivo necesario del Fortimail.

En la Fig. 4.2.10, observamos las especificaciones del requerimiento del Fortimail.

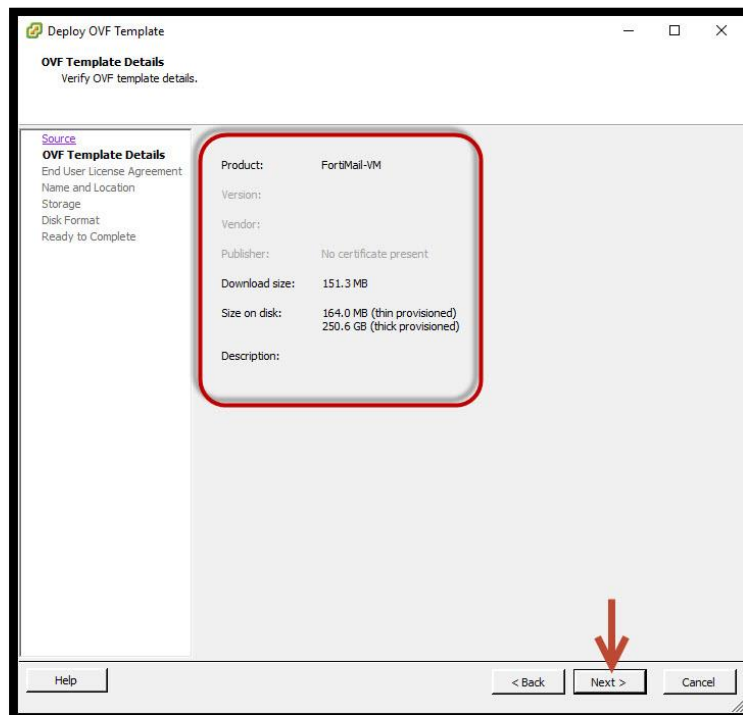


Fig. 4.2.10 Especificaciones del requerimiento del Fortimail.

En la Fig. 4.2.11, evidenciamos la aceptación de la licencia.

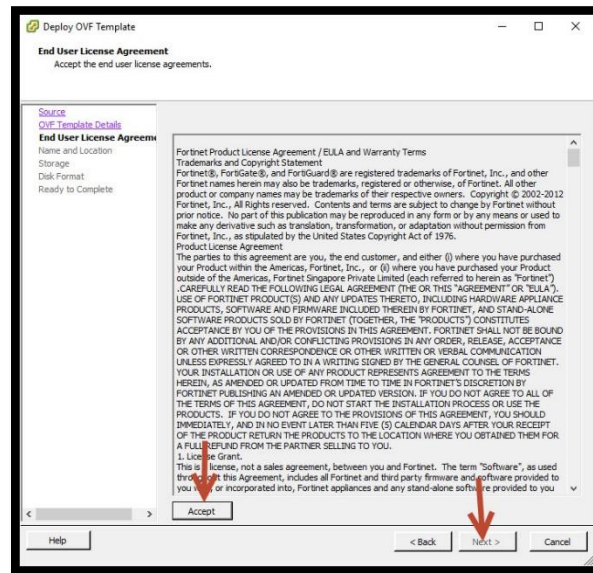


Fig. 4.2.11 Aceptación de la licencia.

En la Fig. 4.2.12, presentamos la configuracion del nombre de la maquina virtual.

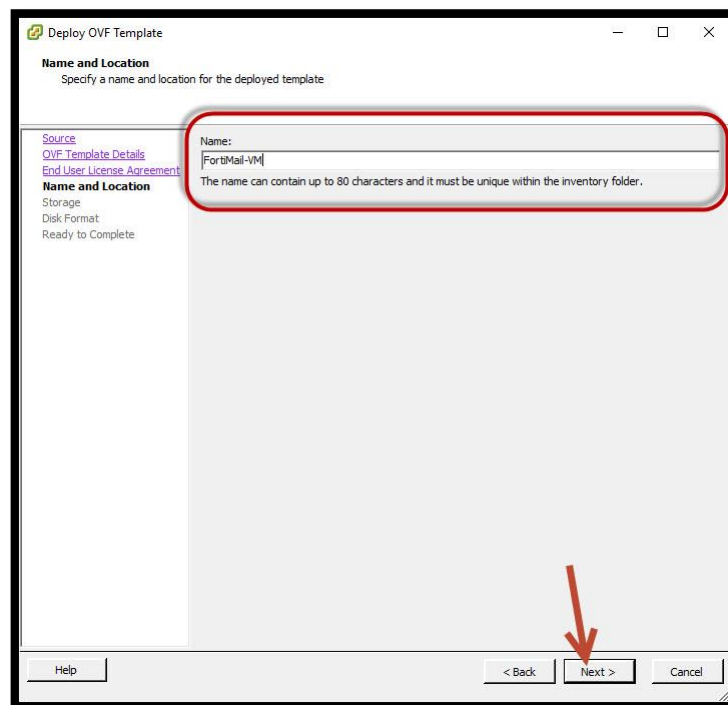


Fig. 4.2.12 Configuración del nombre de la máquina virtual.

En la Fig. 4.2.13, enseñamos el establecimiento del almacenamiento de la maquina virtual.

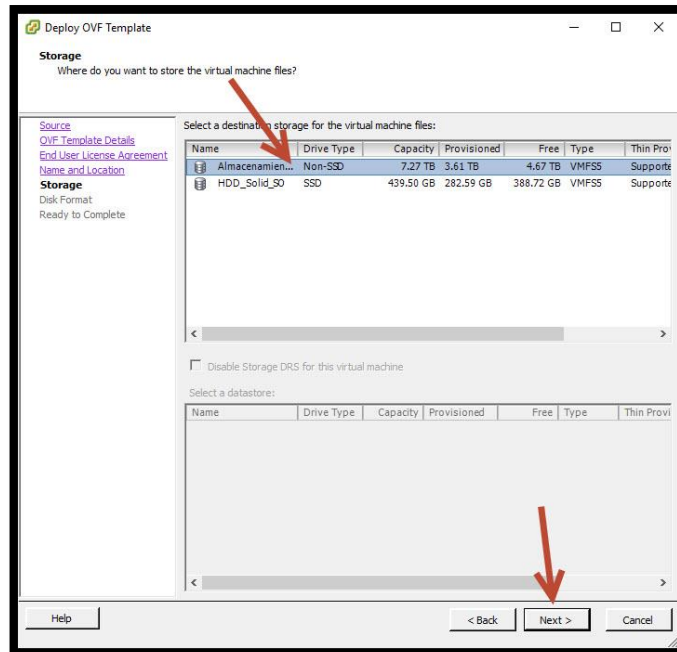


Fig. 4.2.13 Estableciendo el almacenamiento de la máquina virtual.

En la Fig. 4.2.14, observamos la creación del disco virtual VMDK, reservando el espacio definido.

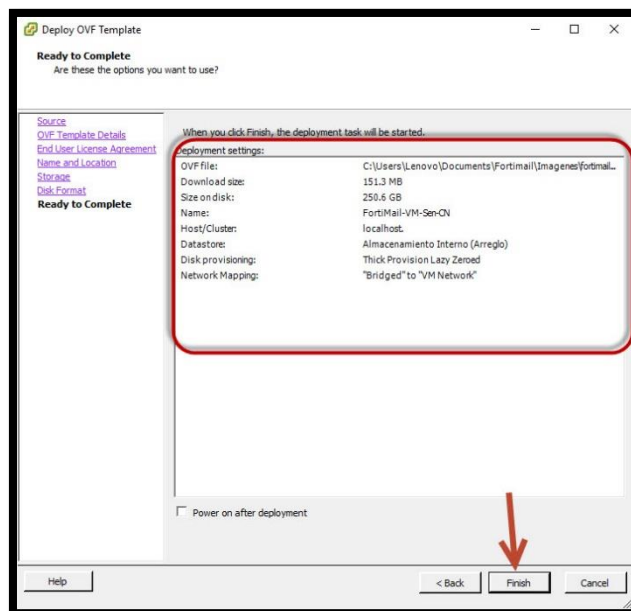


Fig. 4.2.14 Creación del disco virtual VMDK, reservando el espacio definido.



En la Fig. 4.2.15, mostramos el tipo de almacenamiento para el Fortimail.

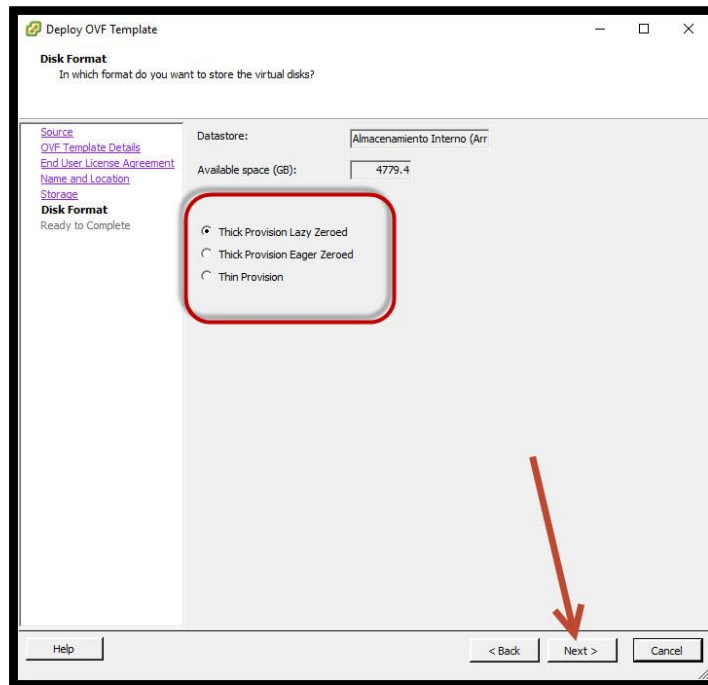


Fig. 4.2.15 Tipo de Almacenamiento para el Fortimail.

Como se ve en la Fig. 4.2.16, indicamos el porcentaje del despliegue de la maquina virtual del Fortimail.

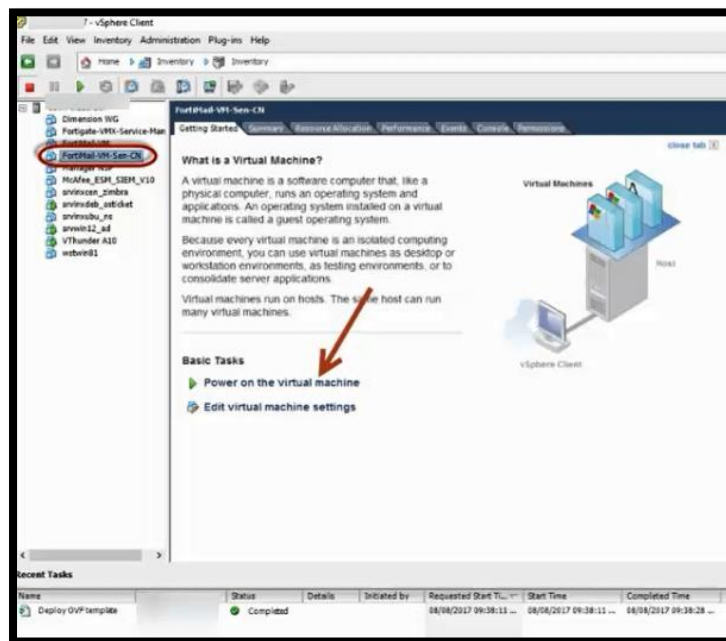


Fig. 4.2.16 Porcentaje del despliegue de la máquina virtual del Fortimail.



### 4.3. Administración de Fortimail.

En la Fig. 4.3.1, presentamos la finalización del despliegue de la máquina virtual.

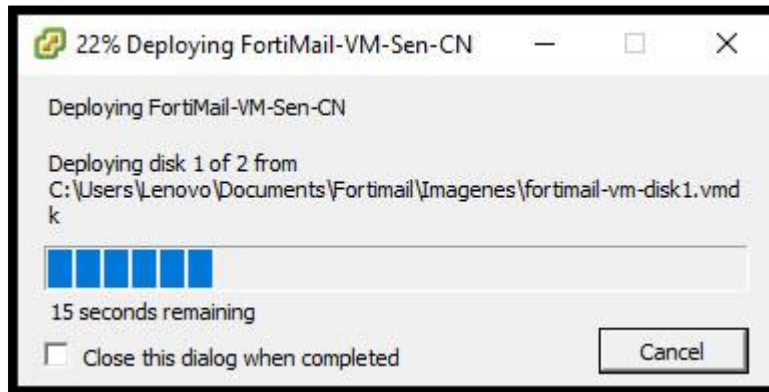


Fig. 4.3.1 Finalización del despliegue de la máquina virtual.

Por defecto el Fortimail tiene una IP que es la: “192.168.1.99” pero como esa IP no nos servirá ya que el equipo es virtual, en cuando lo encendemos le cambiaremos la IP a la que necesitamos desde la consola del Esxi.

Por el tipo de implementación y la arquitectura requerida, la interfaz que configuraremos acá recibirá todo, desde la administración hasta el envío y recepción de correo, análisis, conexión a internet etc. [4]

En la Fig. 4.3.2, observamos el arranque de la máquina virtual del Fortimail.

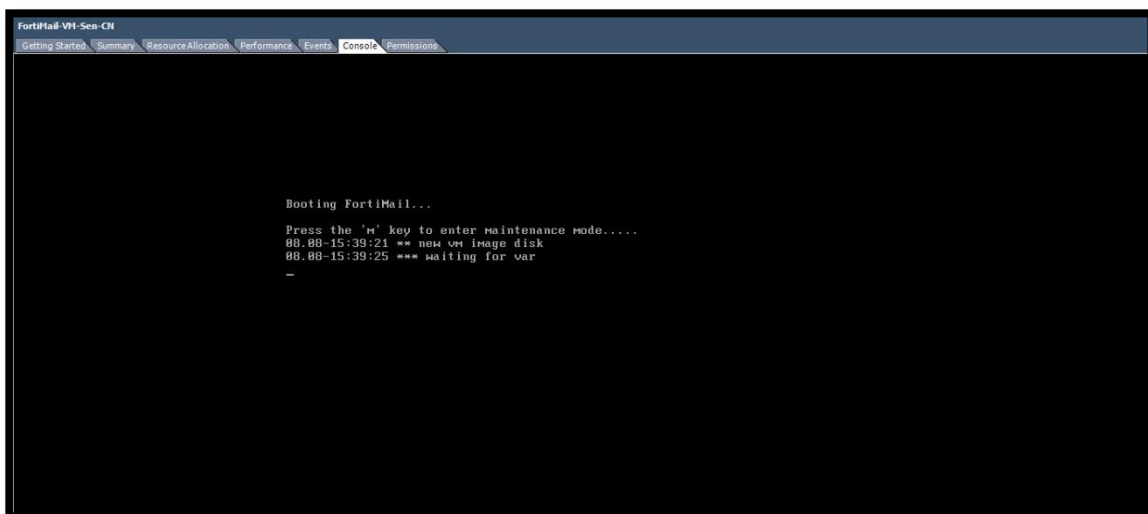


Fig. 4.3.2 Arranque de la máquina virtual del Fortimail.

Luego nos autenticamos, en este punto “el login es: admin y el password: no es nada” como se ve en la Fig. 4.3.3.

```
00.00-15:39:21 ** new vm image disk
00.00-15:39:25 *** waiting for var
00.00-15:39:31 *** waiting for var
00.00-15:39:36 ** partitioning new vm system
enabling LVM
partitioning devices
creating volume group
creating logical devices
starting LVM subsystem
LVM created
00.00-15:39:52 ** formatting system
formatting partition /dev/vga/vga2 as reiserfs...
successful
formatting partition /dev/vga/vga3 as reiserfs...
successful
00.00-15:40:08 *** waiting for var
00.00-15:40:14 *** waiting for var
Initialize Database ...
Initialize Configuration ...
00.00-00:40:29 Parsing default configuration file!

FEUM0000000000 login:
FEUM0000000000 login: _
```

Fig. 4.3.3 Autenticación del Fortimail.

En la Fig. 4.3.4, mostramos el ingreso de las credenciales por defecto.

```
00.00-15:39:31 *** waiting for var
00.00-15:39:36 ** partitioning new vm system
enabling LVM
partitioning devices
creating volume group
creating logical devices
starting LVM subsystem
LVM created
00.00-15:39:52 ** formatting system
formatting partition /dev/vga/vga2 as reiserfs...
successful
formatting partition /dev/vga/vga3 as reiserfs...
successful
00.00-15:40:08 *** waiting for var
00.00-15:40:14 *** waiting for var
Initialize Database ...
Initialize Configuration ...
00.00-00:40:29 Parsing default configuration file!

FEUM0000000000 login:
FEUM0000000000 login: admin
Password:
FEUM0000000000 # _
```

Fig. 4.3.4 Ingresando las Credenciales por defecto.

Luego ejecutamos el siguiente comando:

“config system interface  
edit port 1  
set ip x.x.x.x x.x.x.x”

En la Fig. 4.3.5, exponemos el establecimiento del direccionamiento de IP privada.

```
FEU0000000000 (interface) # set inter
Parsing error at 'set'. err=1

FEU0000000000 (interface) #
edit      add/edit a table value
delete    delete a table value
purge     clear all table value
rename    rename a table entry
get       get dynamic and system information
show      show configuration
end       end and save last config

FEU0000000000 (interface) # end

FEU0000000000 #
FEU0000000000 #
FEU0000000000 #
FEU0000000000 #
FEU0000000000 # config system interface
FEU0000000000 (interface) # edit port1
FEU0000000000 (port1) #
FEU0000000000 (port1) # set ip 0.0.0.0 0.0.0.0_
```

Fig. 4.3.5 Estableciendo el direccionamiento de IP privada de nuestra Empresa.

**Nota:** El Fortimail virtual trae hasta 5 interfaces, la interfaz por defecto es la 1, por eso la configuramos aca, pero igual se puede configurar una interfaz de cada funcion incluso solo de administracion.

Luego de poner la IP, ponemos en el buscador la IP que configuramos con la siguiente direccion: [https://ip\\_fortimail/admin](https://ip_fortimail/admin).

Ahí tendremos que darle una excepcion al navegador por el certificado.

**Nota:** Para quitar ese mensaje podemos exportar el certificado del Fortimail e instalarlo en la PC desde donde se tenga que acceder.

En la Fig. 4.3.6, observamos como entramos en la interfaz gráfica desde el Navegador.

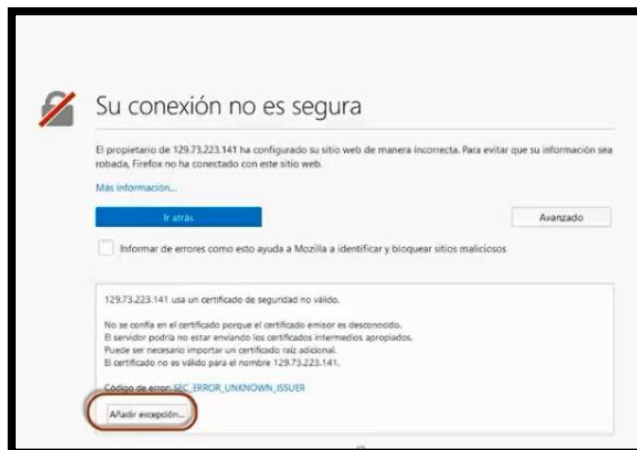


Fig. 4.3.6 Entrando a la Interfaz Gráfica desde el Navegador.

En la Fig. 4.3.7, exhibimos la confirmación de la excepción de seguridad.

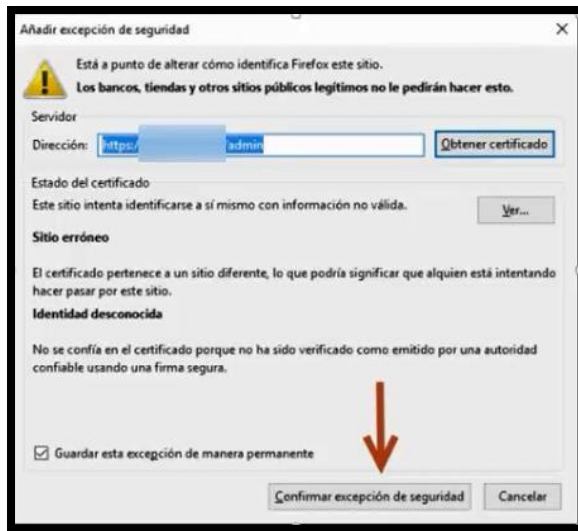


Fig. 4.3.7 Confirmando la excepción de seguridad.

Luego nos autenticamos, recordemos que todavía no tenemos configurado password, así que ese campo lo dejamos en blanco y accedemos a la herramienta.

En la Fig. 4.3.8, observamos el ingreso de las credenciales de administrador.



Fig. 4.3.8 Ingresando las credenciales de administrador en la consola del Fortimail.

En la Fig. 4.3.9, presentamos el acceso a la interfaz gráfica del Fortimail.

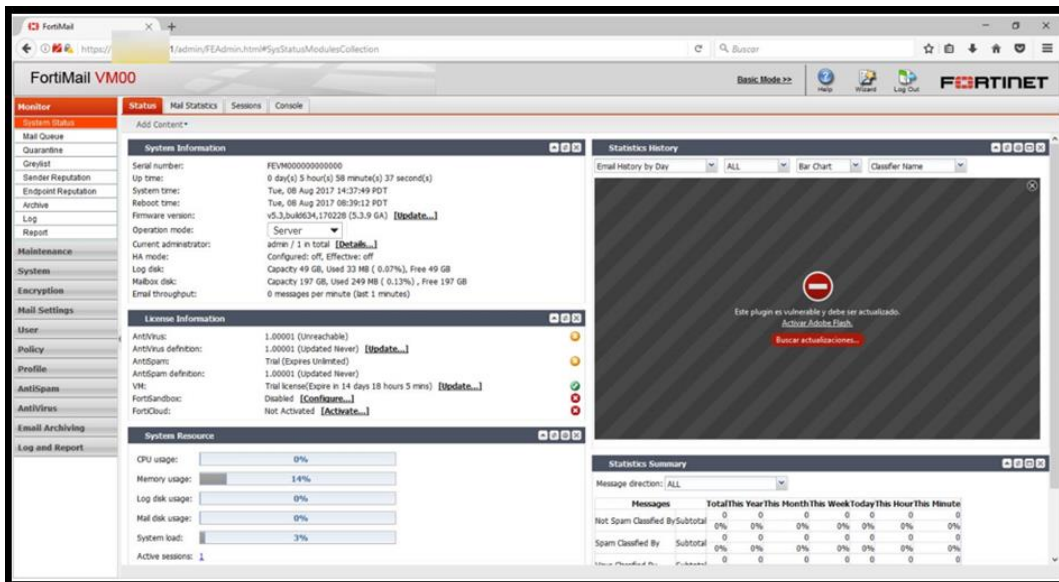


Fig. 4.3.9 Acceso a la interfaz Gráfica del Fortimail.

#### 4.4. Aplicando licencia.

Los primeros 15 días después de instalado el equipo, tendremos una licencia “demo” puesto que no podremos actualizar las firmas, ni acceder a la red de Fortimail en la nube, otra característica desactivada es el Sandbox.

Previamente tuvimos que haber creado una cuenta en la página de Fortinet (Cualquiera puede crear cuenta) y registrar el producto para obtener la licencia.

Para actualizar seguimos la ruta: **Monitor → System Status → Status → VM → Update**

En la Fig. 4.4.1, observamos la interacción con la plataforma del Fortimail.

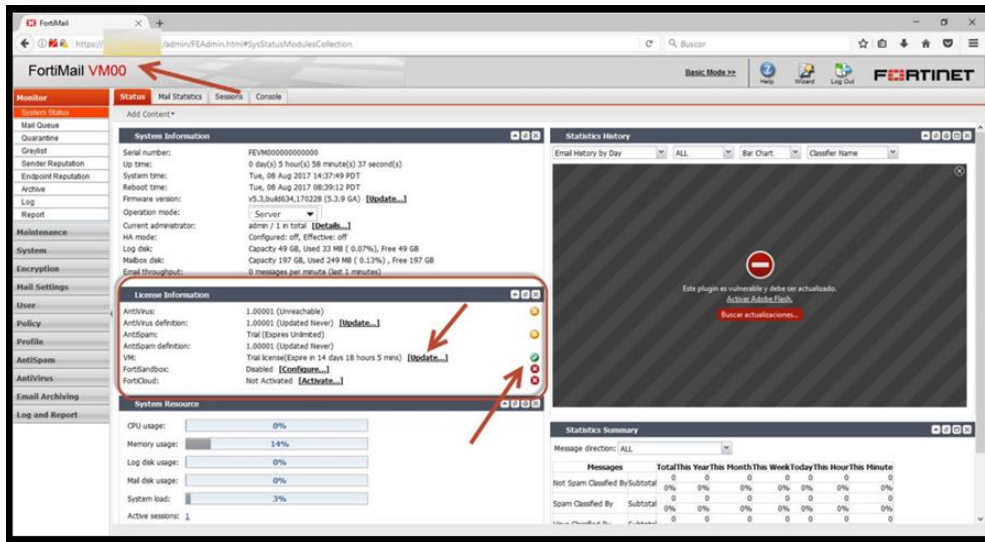


Fig. 4.4.1 Interacción con la consola del Fortimail.

En la Fig. 4.4.2, enseñamos la elección del archivo de licencia:

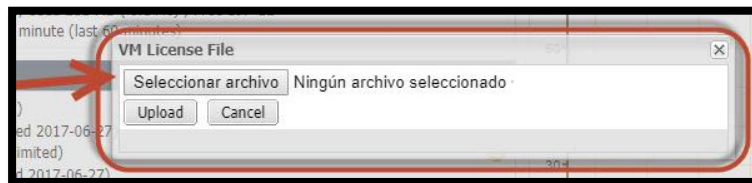
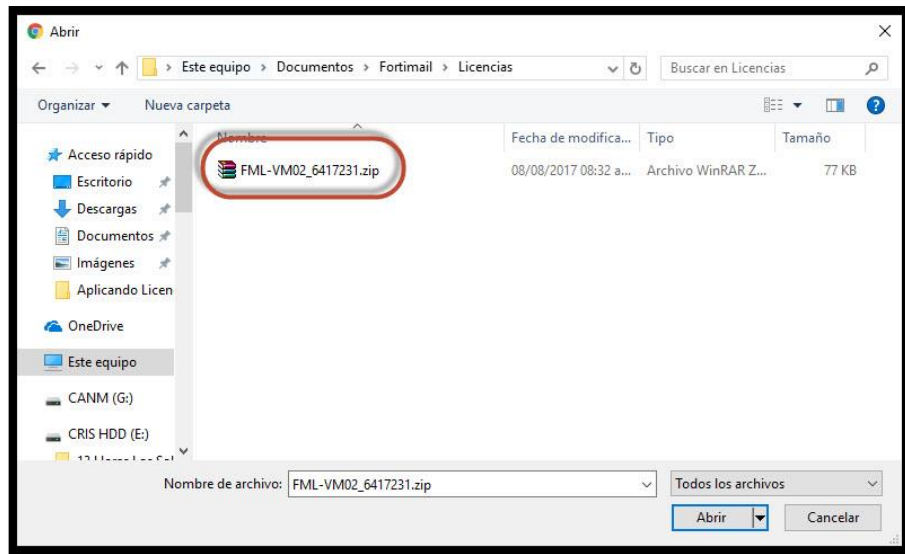


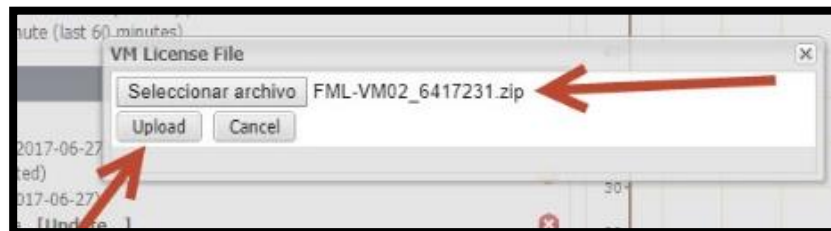
Fig. 4.4.2 Elección del Archivo de Licencia para la consola.

En la Fig. 4.4.3, mostramos la búsqueda del archivo en nuestro ordenador.



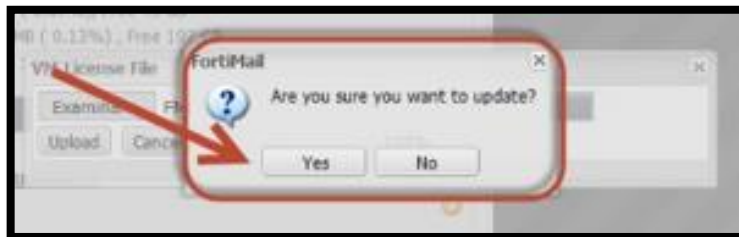
**Fig. 4.4.3 Búsqueda del archivo en nuestro ordenador.**

En la Fig. 4.4.4, indicamos la subida del archivo de licencia a la consola.



**Fig. 4.4.4 Subida del archivo de licencia a la consola.**

En la Fig. 4.4.5, presentamos la confirmación de la actualización por medio del archivo de licencia.



**Fig. 4.4.5 Confirmación de la actualización por medio del archivo de licencia.**

#### 4.5. Configuración Inicial.

Antes de configurar política, tenemos que añadir el dominio a proteger, para esto se deben de tener los siguientes datos:

- IP de donde viene el correo (No precisamente el servidor de correo).
- IP del servidor de correo.
- Dominio.
- Puerto de correo.
- Protocolo de correo.

Cabe destacar que esto se puede hacer no precisamente de este Wizard pero es preferible hacerlo desde aca ya que para configurar las opciones que se necesitan hay que navegar por diferentes lugares del menu del Fortimail y aca estan reunidas y lineales.

En la Fig. 4.5.1, observamos la seleccion del Wizard desde la parte superior derecha:



Fig. 4.5.1 Seleccionando el Wizard de la consola del Fortimail.

Al ejecutar el Wizard nos da una advertencia que si lo ejecutamos borrara las configuraciones que tenga configuradas en esos momentos, como es la primera vez no le prestamos atencion pero hay que considerar que cada vez que corremos el Wizard borrara lo que tiene configurado, no se tiene que hacer en produccion bajo ninguna circunstancia y se tiene que tener respaldo de la configuracion.

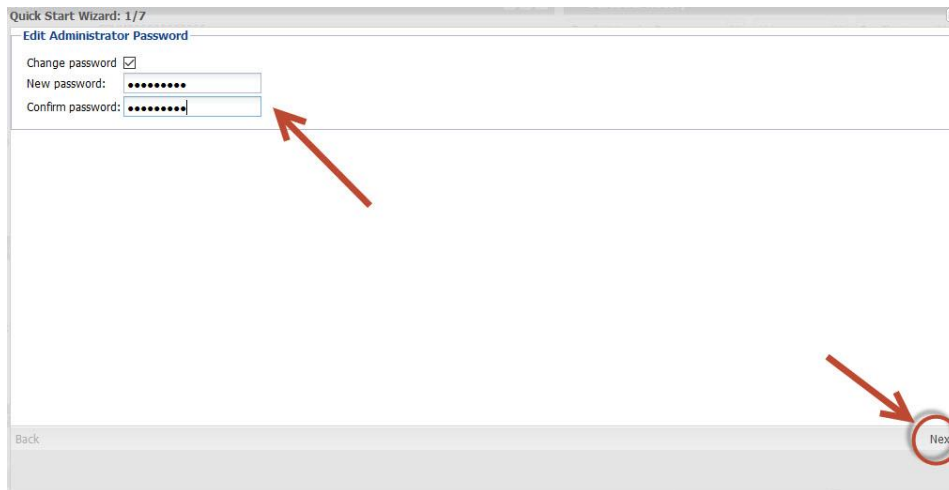
En la Fig. 4.5.2, presentamos la confirmacion del acceso al Wizard del Fortimail.



Fig. 4.5.2 Confirmando el acceso al Wizard del Fortimail.



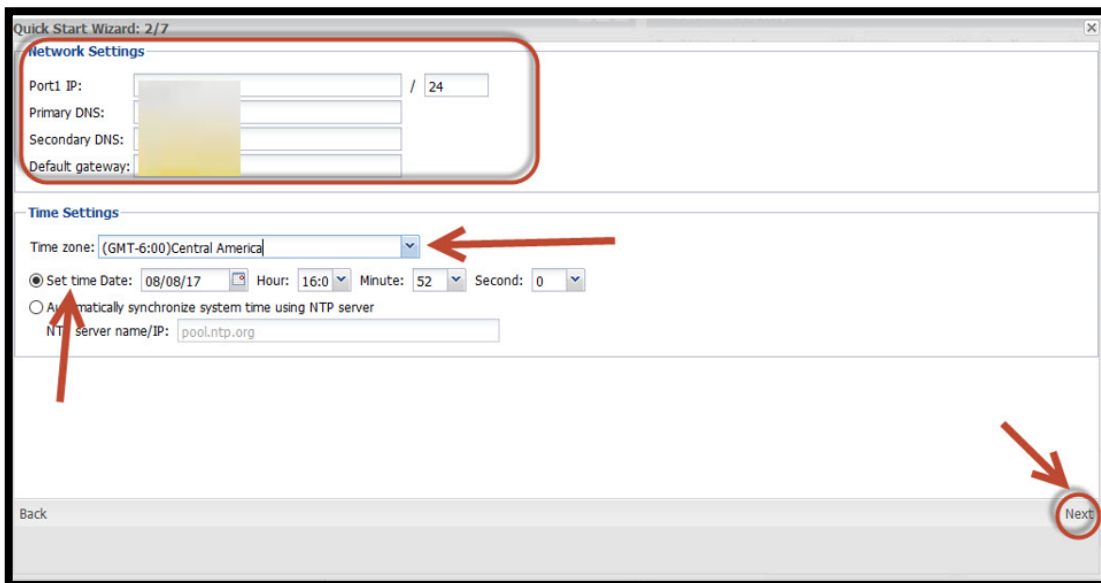
En la Fig. 4.5.3, mostramos el establecimiento de la nueva contraseña de acceso.

The screenshot shows a window titled 'Quick Start Wizard: 1/7' with the subtitle 'Edit Administrator Password'. It contains two input fields: 'New password:' and 'Confirm password:', both with masked characters. A red arrow points from the 'Next' button at the bottom right towards the password fields. The 'Next' button is circled in red.

**Fig. 4.5.3** Estableciendo la nueva contraseña de acceso.

Luego reafirmamos la configuración de Red, y la zona horaria del equipo, esto tiene que estar bien configurado para que la actualización de las firmas sea correcta.

En la Fig. 4.5.4, enseñamos la confirmación de las configuraciones necesarias para el upgrade.

The screenshot shows a window titled 'Quick Start Wizard: 2/7' with two sections: 'Network Settings' and 'Time Settings'. The 'Network Settings' section is highlighted with a red box and contains fields for 'Port1 IP:', 'Primary DNS:', 'Secondary DNS:', and 'Default gateway:'. The 'Time Settings' section contains a 'Time zone:' dropdown menu set to '(GMT-6:00)Central America', and radio buttons for 'Set time Date:' (selected) and 'Automatically synchronize system time using NTP server'. A red arrow points to the 'Next' button at the bottom right, which is circled in red.

**Fig. 4.5.4** Confirmando las configuraciones necesarias para el upgrade.

Luego se tiene que configurar el nombre del equipo, el nombre de dominio y los puertos de correo.

Como se ve en la Fig. 4.5.5, añadimos los puertos de nuestro servidor de correo.

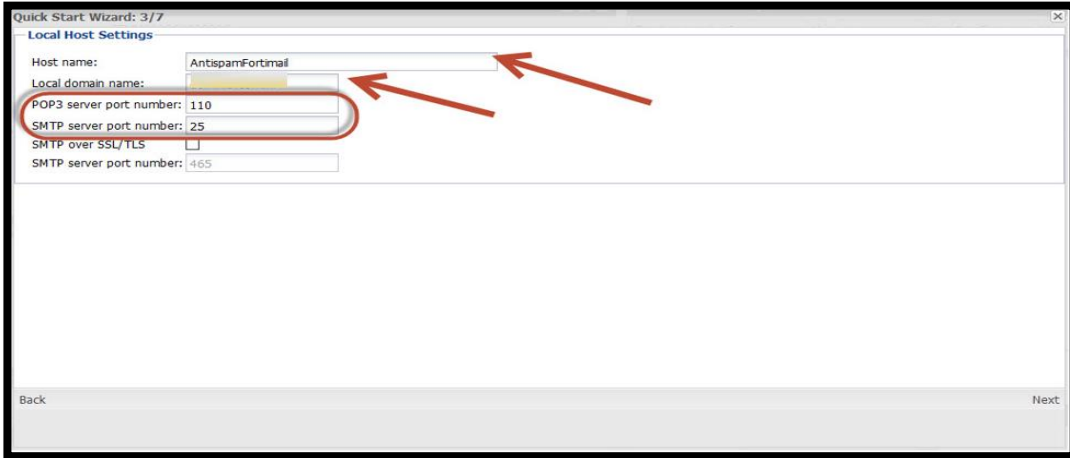


Fig. 4.5.5 Añadiendo los puertos de nuestro servidor de correo.

A continuación mostramos en la Fig. 4.5.6, añadimos el dominio y el gateway de la IP privada.

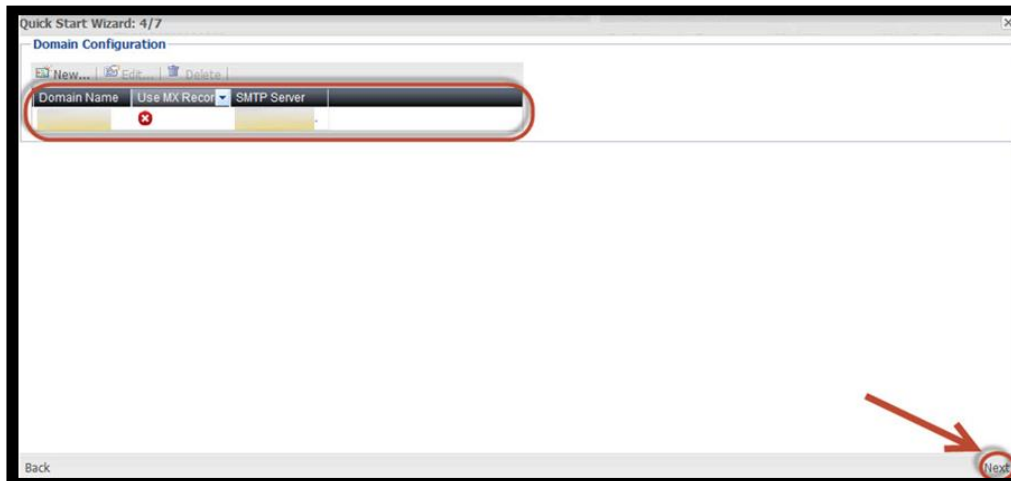


Fig. 4.5.6 Añadiendo nuestro dominio y el Gateway de la IP Privada.

Luego escogemos el nivel de Antispam y Antivirus del Fortimail, esto podemos modificarlo más adelante.

En la Fig. 4.5.7, mostramos la configuración del Antispam.

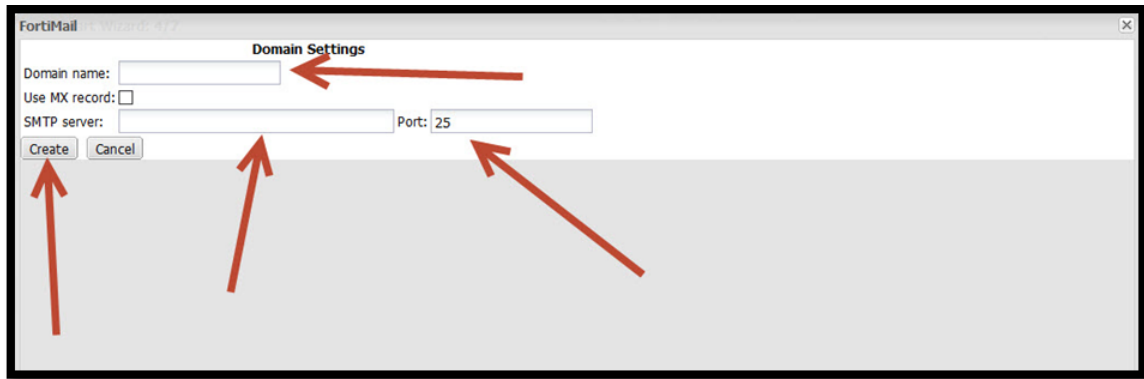


Fig. 4.5.7 Configuración inicial del Antispam.

En la Fig. 4.5.8, observamos la elección del nivel de escaneo del Antispam.

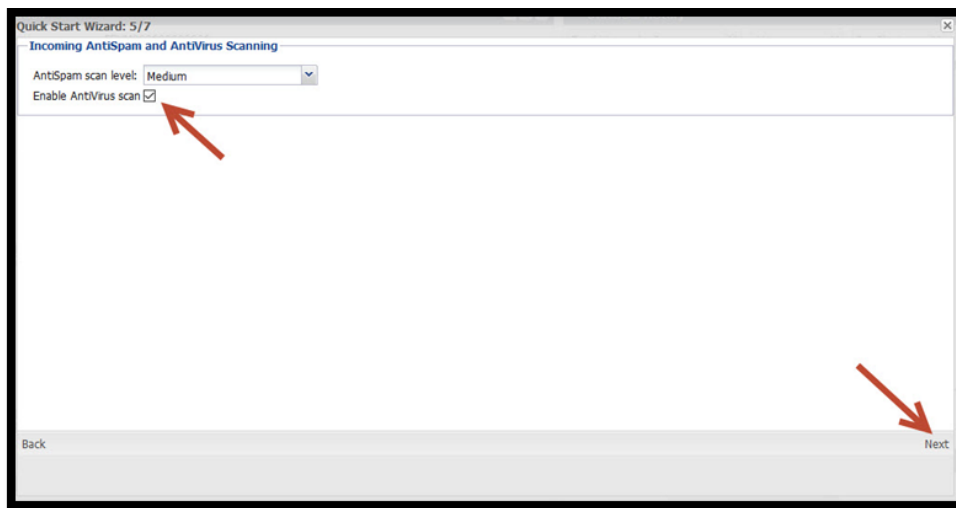


Fig. 4.5.8 Elección del nivel de Escaneo del Antispam.

Como se ve en la Fig. 4.5.9, creamos la política principal de acceso, en la que protegemos el dominio, de cualquier spoofing:

FortiMail - Wizard: 5/7

**Access Control Rule**

Enabled ☒ 0.0.0.0 / 0

Sender pattern: User Defined \*

Recipient pattern: User Defined \*

Sender IP/netmask: Reverse DNS pattern: \*

Authentication status: Any Action: Reject

Comments:

Create Cancel

Fig. 4.5.9 Creación de política principal de Acceso.

En la Fig. 4.5.10, enseñamos el establecimiento del dominio del antispam e ingresamos la IP de donde nos vendrán los correos, igualmente establecemos el dominio del cual vamos a hacer relay y hacia dónde va el correo:

FortiMail - Wizard: 5/7

**Access Control Rule**

Enabled ☒ / 32

Sender pattern: User Defined \*

Recipient pattern: User Defined \*

Sender IP/netmask: Reverse DNS pattern: \*

Authentication status: Any

Action: Not Authenticated Authenticated

Comments: Any

Create Cancel

Fig. 4.5.10 Estableciendo el Dominio al Antispam.

En la Fig. 4.5.11, presentamos el establecimiento de la política de acceso y la acción a tomar de Relay. (Cabe destacar que si el correo es en saliente el estado de la autenticación es siempre “Authenticated” ya que si no es así, es que tenemos alguna PC Botnet o algún spoofing dentro del dominio.

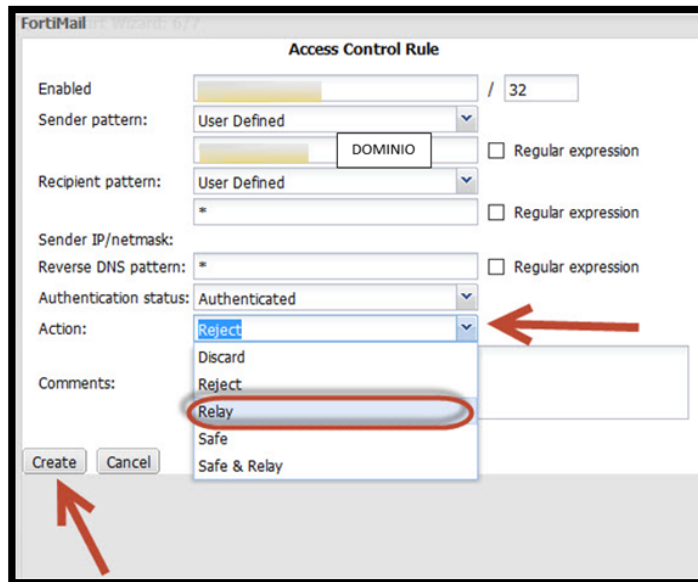


Fig. 4.5.11 Estableciendo en la política de acceso y la acción a tomar de Relay.

La acción a tomar cuando encontremos esta comunicación debería ser “relay” si cumple con lo dispuesto antes, cabe destacar que podemos rechazar el correo en este caso, así mismo permitir otras direcciones específicas desde la cuales necesitemos enviar correos.

En la Fig. 4.5.12, observamos la finalización de la configuración del wizard.

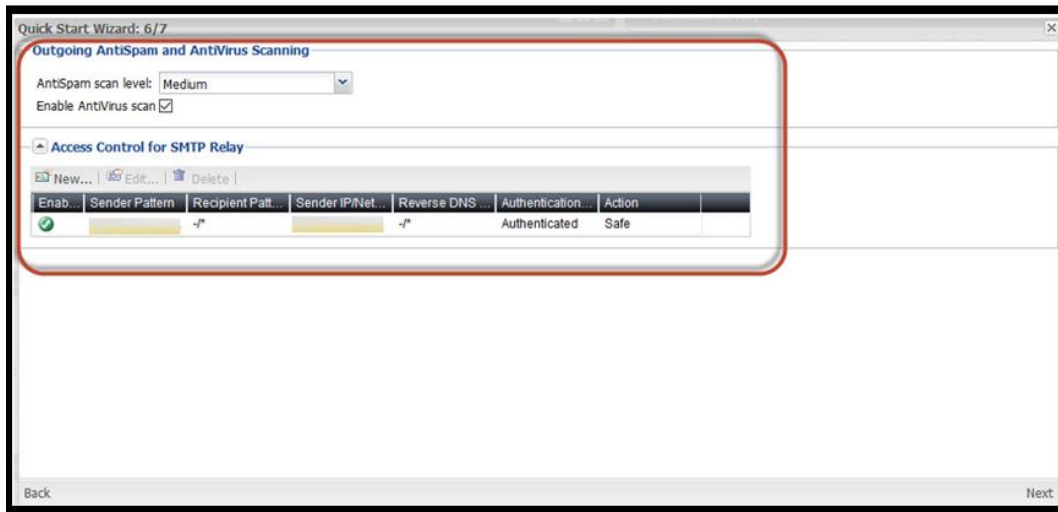


Fig. 4.5.12 Finalizando la configuración del Wizard.

En la Fig. 4.5.13, mostramos el resumen general de la regla de la política de acceso.

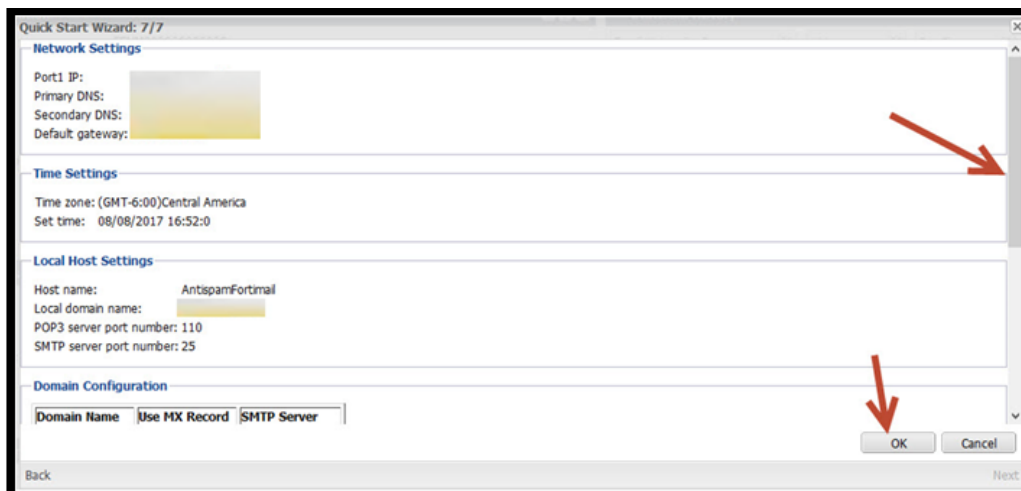


Fig. 4.5.13 Resumen general de la regla de la política de acceso.

Al terminar nos dará un resumen de lo que hemos hecho:

Luego el wizard termina y entonces nos redirigirá a la pantalla de autenticación donde ingresaremos con la nueva contraseña configurada:

En la Fig. 4.5.14, presentamos la pantalla de autenticación del Fortimail con el cambio realizado.

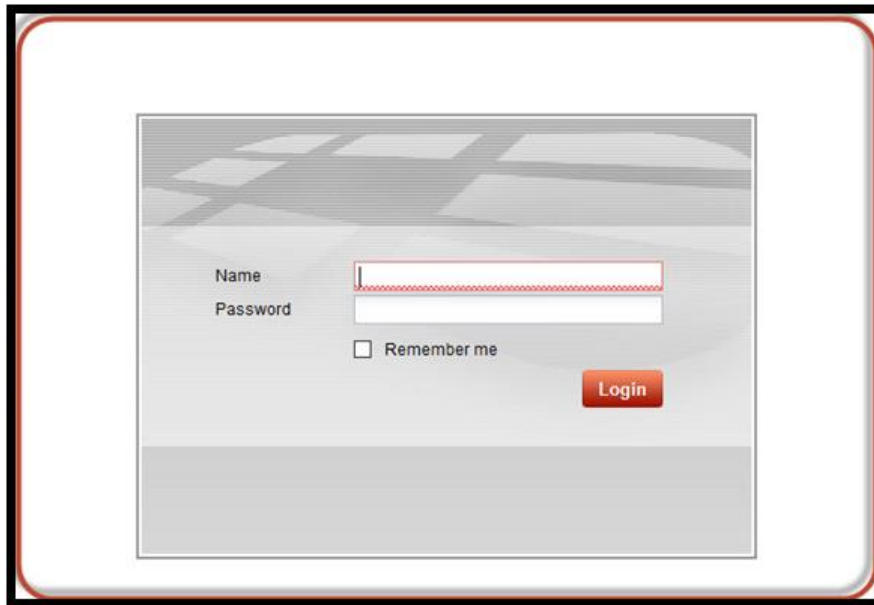


Fig. 4.5.14 Regresando con las nuevas credenciales y políticas establecida.

#### 4.6. Creando Perfiles del Fortimail.

Antes de las políticas debemos configurar los perfiles que se le aplicaran a las políticas, las políticas en general se componen de perfiles que se aplican a origen-destino sin importar si las aplicamos por IP, dominio, usuario.

Los perfiles que podemos configurar vienen desde controlar detalles de las sesiones como los tamaños de correos, como grupos de IP y de correos para permisos especiales, en este documento solo mencionaremos los que se configuraron para Sencom.

Para configurar los perfiles, iremos a la siguiente ruta: **Menú → Profile:**

En esta Fig. 4.6.1, observamos la configuración de los perfiles.



Fig. 4.6.1 Configuración de los perfiles.

Acá podemos elegir entre varios perfiles a configurar, los más importantes y los que ocuparemos por ahora serían:

1. Session
2. Antispam
3. Antivirus
4. Content
5. Notification

#### 4.7. Perfil Session.

Este perfil se aplica a nivel de IP antes de que la conexión SMTP, esto quiere decir que aplica las políticas antes de podamos ver las cuentas de correo, dominio, asunto, etc. Lo que podremos ver en el log solo es la dirección IP y el nombre del servidor de correo de donde viene.

Por esta razón en esta parte solo configuramos el tamaño del correo, dependiendo de las necesidades de los usuarios y las políticas de la empresa, así que creamos un perfil nuevo:



Ponemos un nombre al perfil y configuramos el tamaño del correo en la siguiente dirección: **Profile → Session → New → SMTP Limits → Cap message size (KB)** at, al terminar damos clic en **Create**

En la siguiente Fig. 4.7.1, mostramos el establecimiento del perfil de sesión.

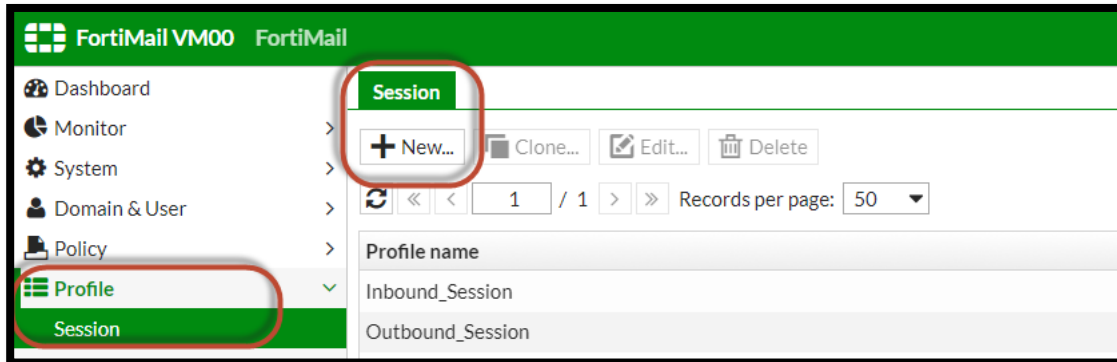


Fig. 4.7.1 Estableciendo el perfil de sesión.

Como se ve a continuación en la Fig. 4.7.2, la creación de la política de sesión.

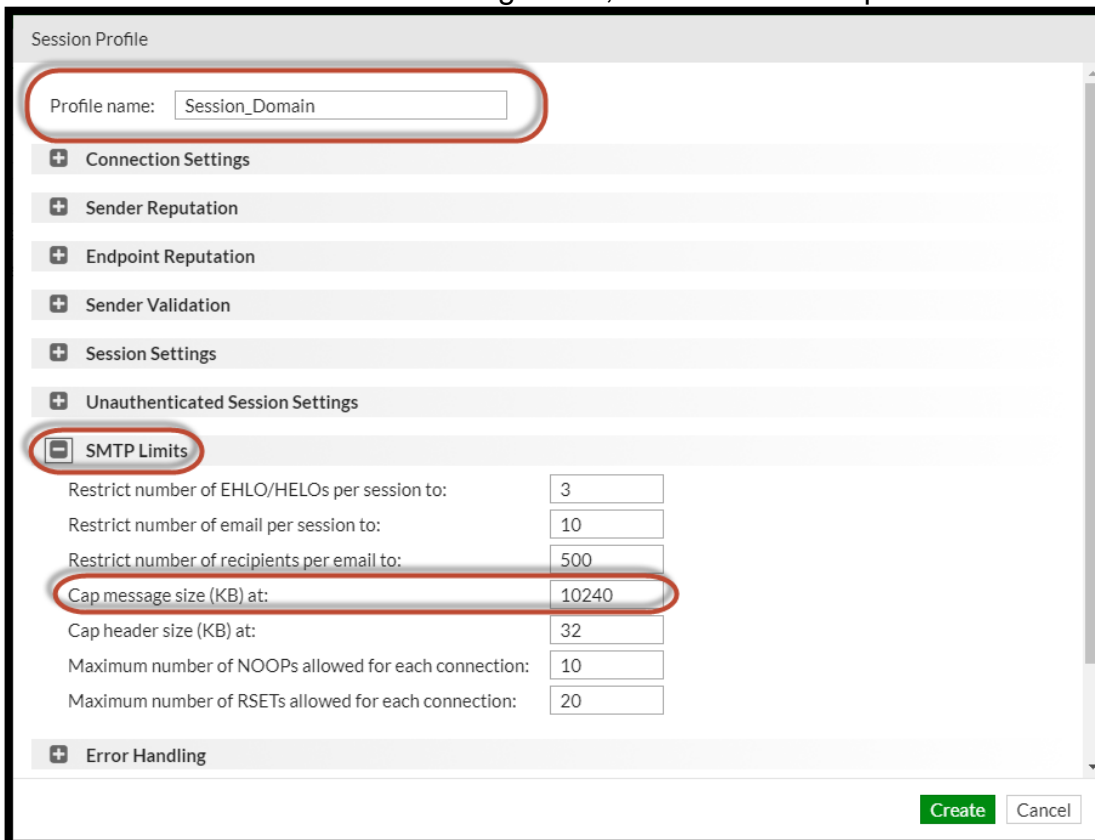


Fig. 4.7.2 Creación de la política de sesión.

En la Fig. 4.7.3, exponemos la confirmación de la política de sesión.

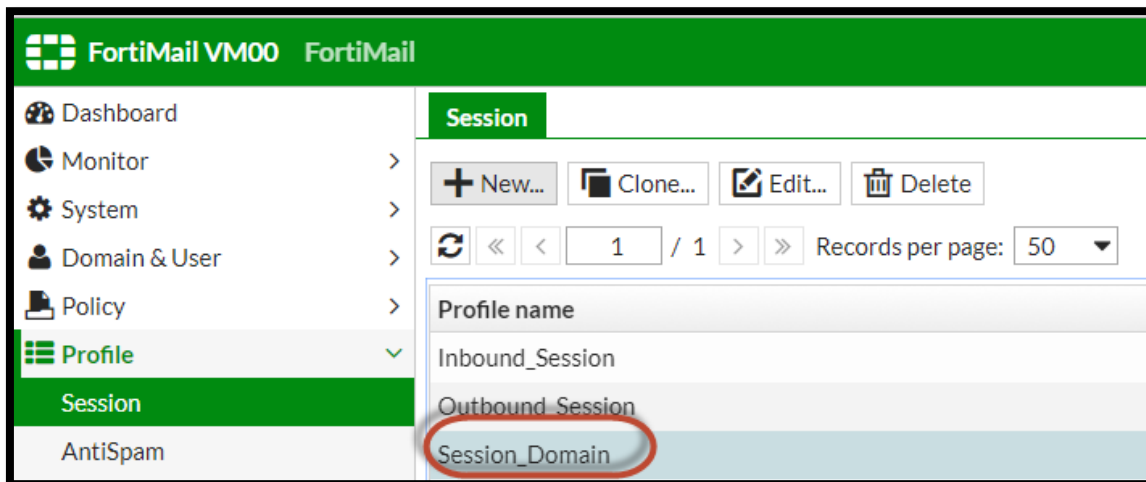


Fig. 4.7.3 Confirmación de la política de sesión.

#### 4.8. Perfil Antispam.

Este perfil es el que marca cómo será la inspección SMTP de los correos, esto puede ser de manera entrante y saliente.

En la Fig. 4.8.1, observamos el panel del antispam ya con la licencia.

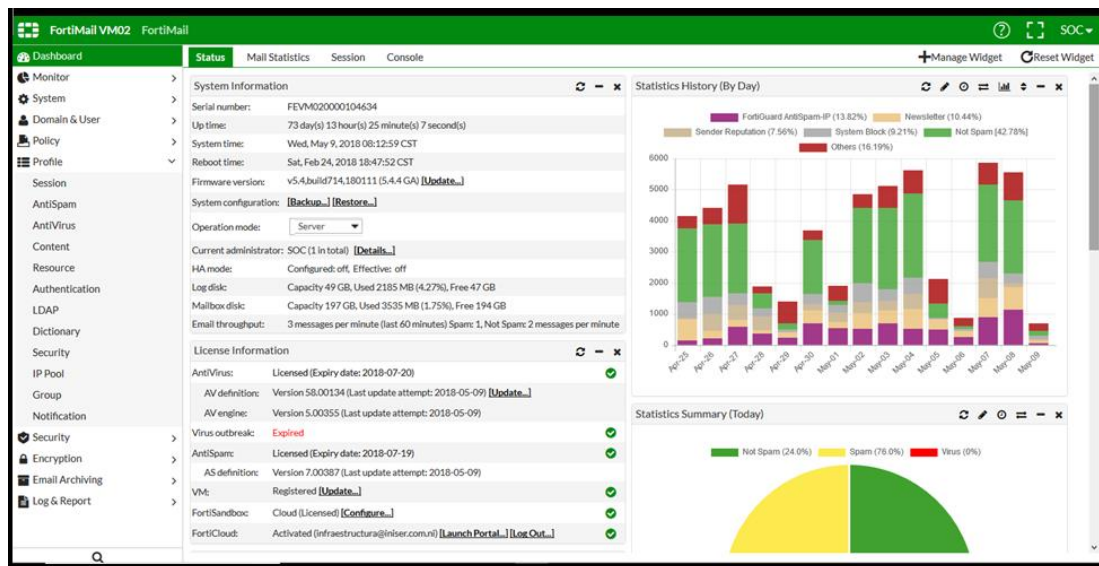


Fig. 4.8.1 Panel del Antispam.

En la Fig. 4.8.2, presentamos la configuración del perfil del antispam.

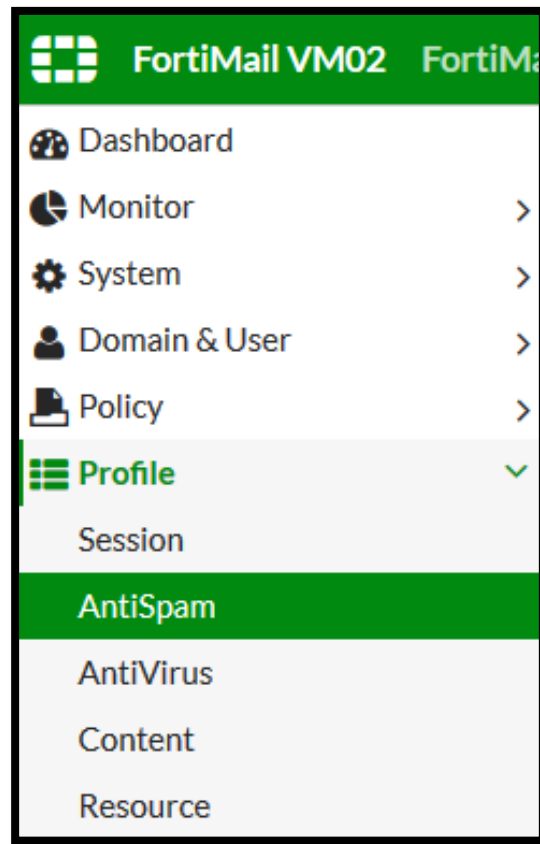


Fig. 4.8.2 Configuración del perfil de Antispam.

Creando los perfiles del Antispam, damos click en new y luego configuramos el perfil de entrada y salida.

Como se ve en la Fig. 4.8.3, creamos el perfil del antispam en la entrada.

AntiSpam Profile

Domain: --System--

Profile name: Incoming\_Antispam

Default action: Incoming\_Antispam + New... Edit...

**Scan Configurations**

Configuration	Action
<input checked="" type="checkbox"/> FortiGuard	Incoming_Antispam
<input type="checkbox"/> Greylist	--Default--
<input type="checkbox"/> SPF check	--Default--
<input type="checkbox"/> DMARC check	Incoming_Antispam
<input checked="" type="checkbox"/> Behavior analysis	Incoming_Antispam
<input checked="" type="checkbox"/> Header analysis	Incoming_Antispam
<input checked="" type="checkbox"/> Heuristic	Incoming_Antispam
<input checked="" type="checkbox"/> SURBL [Configuration...]	--Default--
<input checked="" type="checkbox"/> DNSBL [Configuration...]	--Default--
<input checked="" type="checkbox"/> Banned word [Configuration...]	--Default--
<input checked="" type="checkbox"/> Safelist word [Configuration...]	--Default--
<input checked="" type="checkbox"/> Dictionary	--Default--
<input checked="" type="checkbox"/> Image spam	--Default--
<input checked="" type="checkbox"/> Bayesian	--Default--
<input checked="" type="checkbox"/> Suspicious newsletter	Incoming_Antispam
<input checked="" type="checkbox"/> Newsletter	Incoming_Antispam

**Scan Options**

Max message size to scan: 600 KB (0 means no limits)

☐ Bypass scan on SMTP authentication

☒ Scan PDF attachment

☒ Apply default action without scan upon policy match

OK Cancel

Fig. 4.8.3 Perfil del Antispam en la entrada.

A continuación en la siguiente Fig. 4.8.4, observamos el perfil de salida del Antispam.

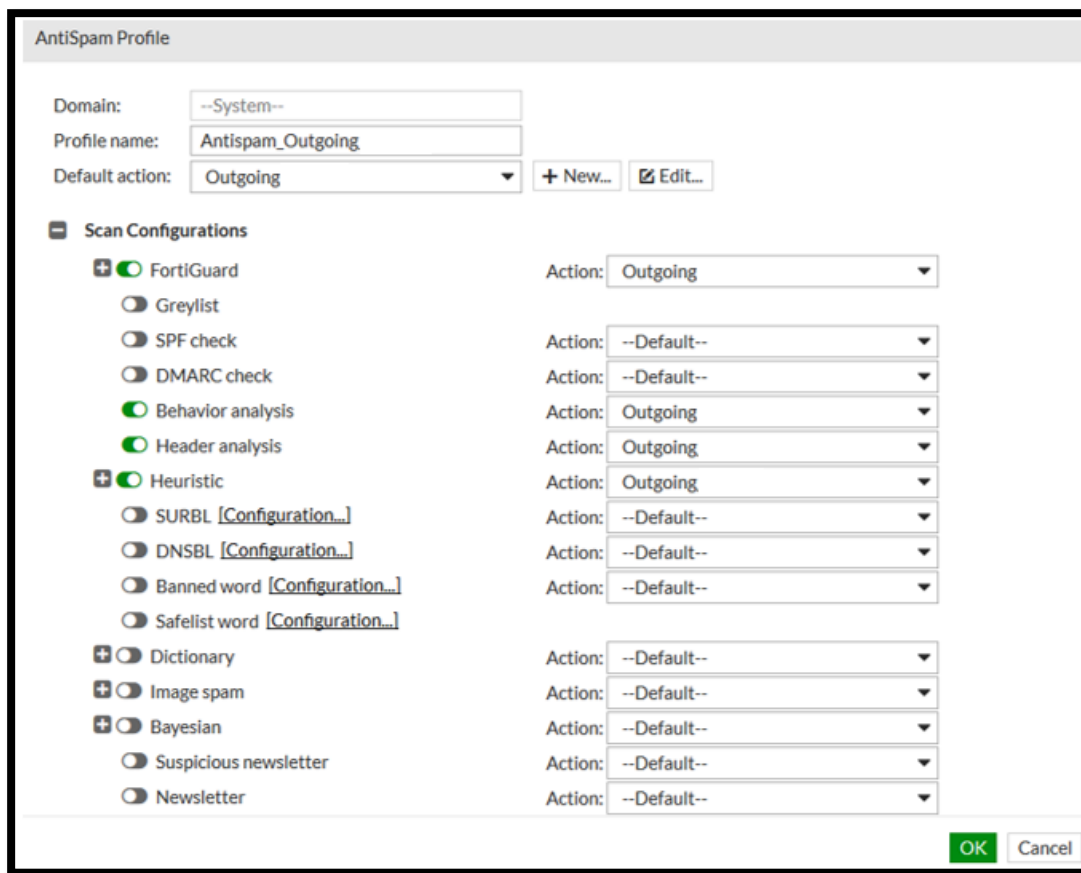


Fig. 4.8.4 Perfil de Salida del Antispam.

Como se ve en la Fig. 4.8.5, creación de las políticas tanto entrante como saliente.

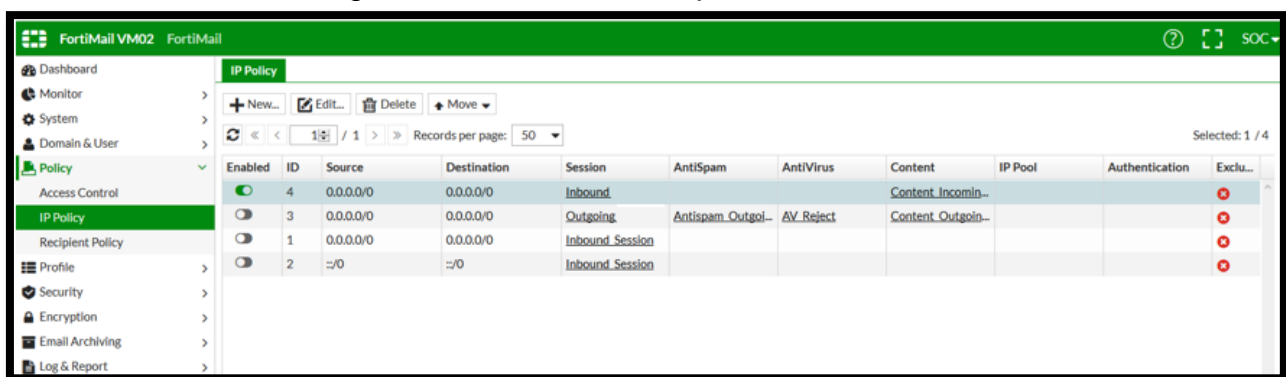


Fig. 4.8.5 Política tanto entrante como saliente.

Al igual que el perfil del AntiSpam el perfil de contenido examina también el protocolo SMTP de los correos para los distintos archivos que son enviados.

En la Fig. 4.8.6, observamos el perfil de contenido de entrada.

Content Profile

Domain: system

Profile name: Content\_Incoming

Action: Content\_Incoming [New...] [Edit...]

**Attachment Scan Rules**

[New...] [Edit...] [Delete] [Move]

Enabled	File Filter	Operator	Action
<input checked="" type="checkbox"/>	executable_windows	Is	--Default--
<input type="checkbox"/>	video	Is	--Default--
<input type="checkbox"/>	audio	Is	--Default--
<input type="checkbox"/>	image	Is	--Default--
<input type="checkbox"/>	archive	Is	--Default--
<input type="checkbox"/>	encrypted	Is	--Default--

**Scan Options**

☐ Bypass scan on SMTP authentication

Fig. 4.8.6 Perfil de Contenido de Entrada.

En la Fig. 4.8.7, enseñamos la continuación del perfil de contenido.

☒ Detect fragmented email

☒ Detect password protected Office document

☐ Attempt to decrypt PDF document

☒ Detect embedded component

☒ MS Office

☒ Visual Basic for Application

☒ MS Visio

☒ Open Office

☐ PDF

☐ Defer delivery of message on policy match

☐ Defer delivery of message larger than 0 KB

☐ Maximum number of attachment 10

☐ Maximum size message 10240 KB

Action: --Default--

☐ Adult image analysis

Action: --Default--

Fig. 4.8.7 Continuación del Perfil de contenido.

En la Fig. 4.8.8, presentamos la finalización del perfil de contenido.

The screenshot shows the 'Content Disarm and Reconstruction' configuration window in FortiMail. It is divided into three main sections:

- Content Disarm and Reconstruction:**
  - Action: --Default--
  - HTML content: ☒ Convert HTML to text
  - Remove URIs: ☐
  - MS Office: ☐ (with a warning icon)
  - PDF: ☐ (with a warning icon)
- Archive Handling:**
  - Check archive content: ☒
  - Detect on failure to decompress: ☒
  - Detect password protected archive: ☒
  - Attempt to decrypt archive: ☐
  - Max level of compression: 12
- File Password Decryption Options:**
  - Words in email content: ☒
    - Number of words to try: 5
  - Built-in password list: ☐
  - User-defined password list: ☐

At the bottom right, there are 'OK' and 'Cancel' buttons.

Fig. 4.8.8 Finalización del Perfil de Contenido.

Bien al ser una interfaz virtual es necesario establecerlo con el dirección privado asignado.

Como se ve en la Fig. 4.8.9, configuramos el antispam.

The screenshot shows the FortiMail VM02 configuration interface. The 'Network' tab is selected, displaying a table of network interfaces. The table has columns for Name, Type, IP/Netmask, IPv6/Netmask, Access, Status, and a Total column. One interface, 'port1', is listed with a Physical type and a status of 'up'.

Name	Type	IP/Netmask	IPv6/Netmask	Access	Status	Total
port1	Physical		:::0	HTTPS,PING,SSH	up	

Fig. 4.8.9 Configuración del Antispam.

Ahora configuramos la lista negra son todos aquellos nombres de dominios, diferentes páginas web que envíen correos no deseado y las listas blancas son todos aquellos dominios que necesitamos acceso por correo.

A continuación veremos en la siguiente Fig. 4.8.10, configuramos las lista negra o blanca.

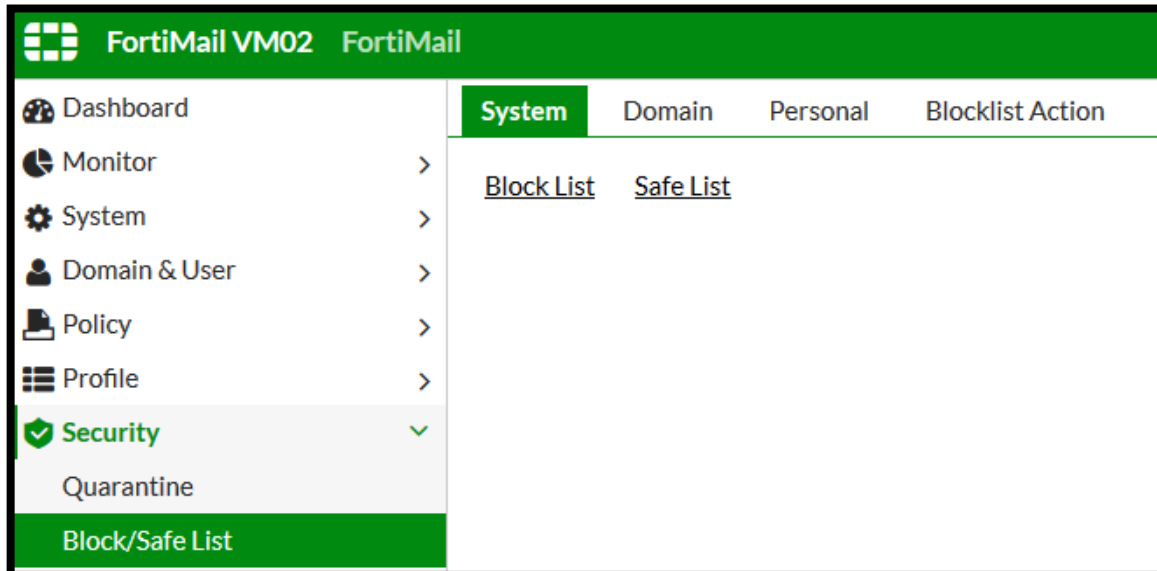


Fig. 4.8.10 Configuración de lista negra o blanca.



En la Fig. 4.8.11, observamos la lista blanca.

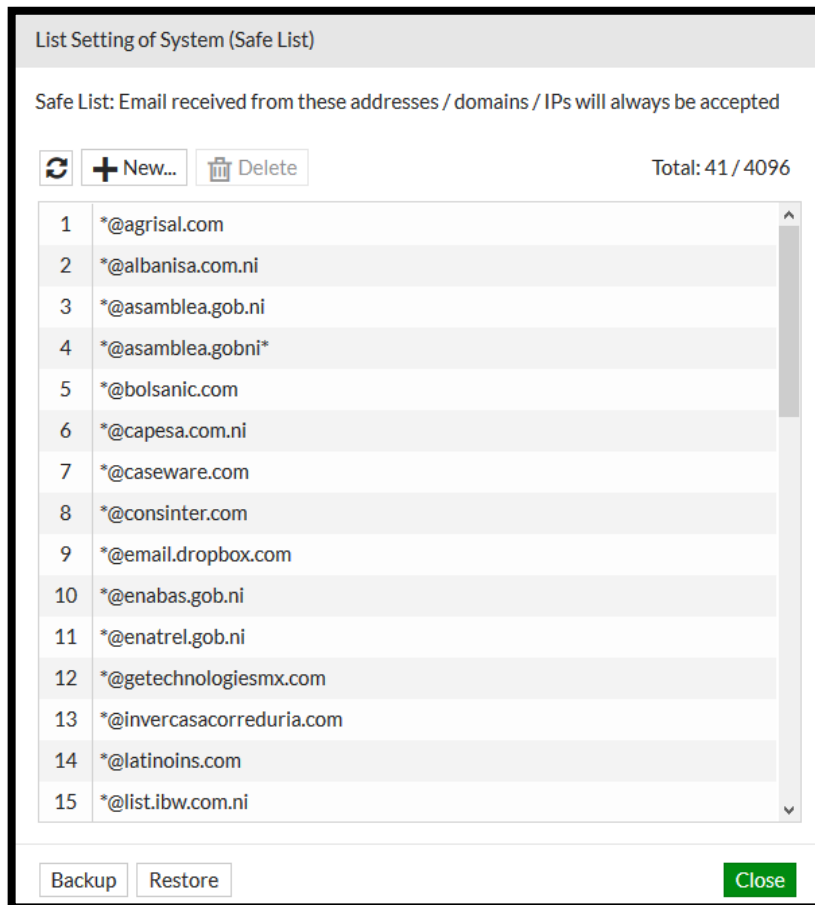
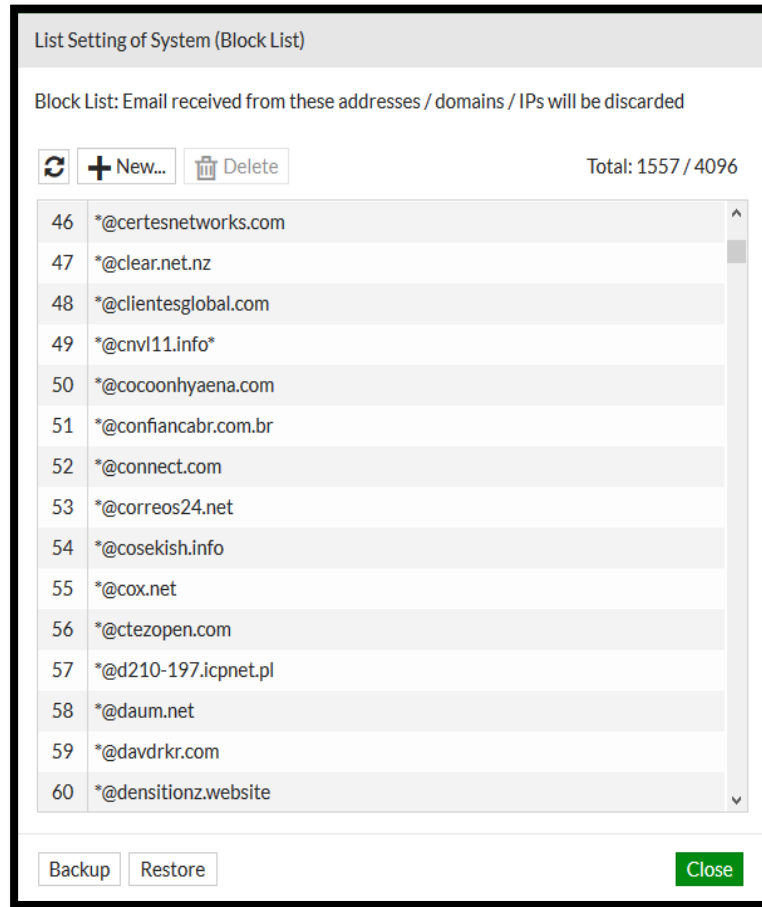


Fig. 4.8.11 Lista Blanca.

En la Fig. 4.8.12, mostramos la lista Negra.



**Fig. 4.8.12 Lista Negra.**

#### 4.9. SURBI

SURBL (anteriormente conocido como Spam URI RBL) es una colección de listas URI DNSBL de hosts de Identificador uniforme de recursos (URI), generalmente dominios de sitios web, que aparecen en mensajes no solicitados. SURBL se puede utilizar para buscar cuerpos de mensajes de correo electrónico entrantes para enlaces de carga útil de correo no deseado para ayudar a evaluar si los mensajes no son solicitados.

En esta Fig. 4.9.1, presentamos los sitios web con envíos de correo no deseado.

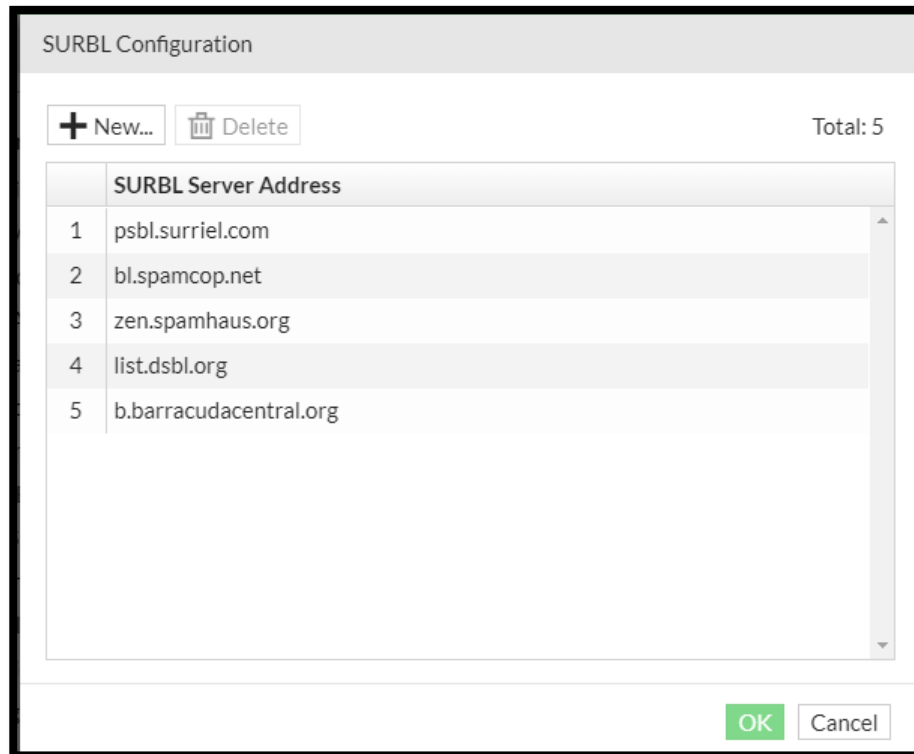


Fig. 4.9.1 Sitios Web con envíos de correo no deseado.

## Capítulo 5

### 5. DMZ

#### 5.1. Teoría

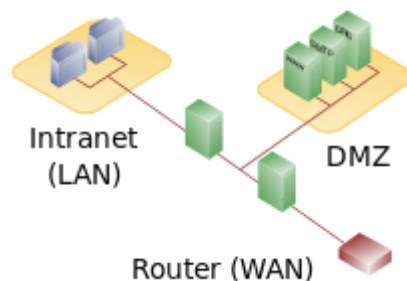
A como es de saber uno de los objetivos de nuestra monografía es la implementación de una zona DMZ (zona desmilitarizada) en la red de la empresa Systems Enterprise S.A, primeramente discutiremos algunas preguntas introductorias como lo son:

¿Qué es una DMZ? Y para que nos servirá en nuestra red y en nuestra seguridad.

Una DMZ o zona desmilitarizada básicamente es una zona insegura en nuestra red, a la cual se debe tener acceso desde el internet (WAN) y nuestra zona segura (LAN), pero con la condición de que nuestros equipos en la zona DMZ no tengan acceso a nuestra LAN, por lo cual generalmente se tienen separadas, esto siempre con el objetivo de garantizar la mayor seguridad a nuestra LAN.

Esta zona desmilitarizada nos servirá para poder aislar nuestros servicios publicados o con acceso desde el Internet de nuestra red segura, y así poder evitar la posibilidad de que ataques destinados a estos servicios nos perjudiquen. [5]

En la Fig. 5.1.1 exhibimos el esquema de la zona DMZ.



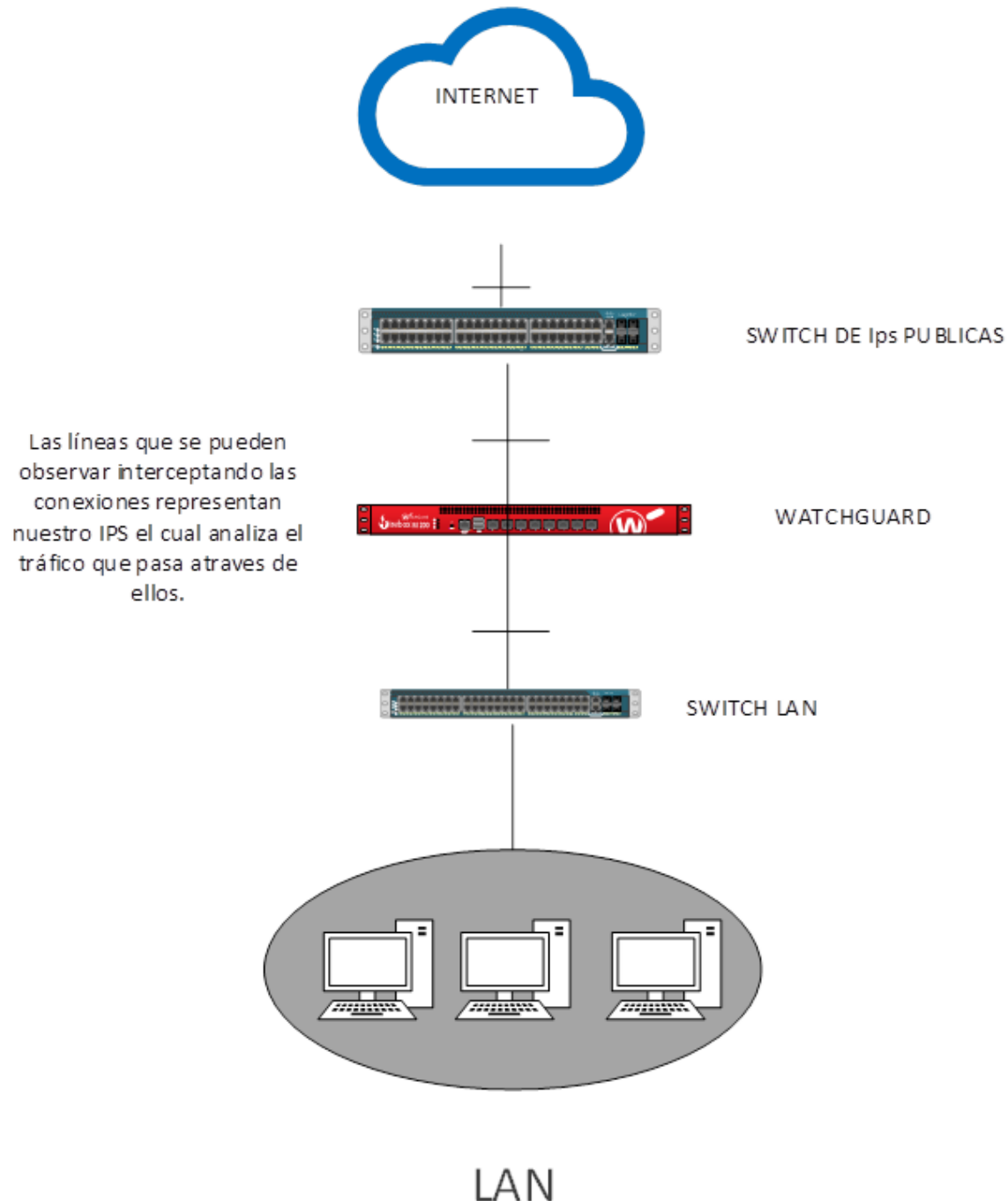
**Fig. 5.1.1 Esquema de la Zona DMZ.**

Para poder entender mejor la implementación de nuestra zona DMZ se observaran dos diagramas, uno describirá como se tiene la red anteriormente a la propuesta, y luego como quedo la red después de nuestra implementación.

Nota: los diagramas que serán mostrados serán hechos superficialmente con el propósito del entendimiento de la estructuración de esta zona. [2]

En la Fig. 5.1.2, observamos el esquema antes de la implementación de la zona DMZ.

**Diagrama sin zona DMZ.**



**Fig. 5.1.2 Esquema Antes de la implementación de la Zona DMZ.**

A como se puede observar la topología de red anterior nos muestra la estructura básica de nuestra red, en donde se ve nuestros watchguard administrando el tráfico proveniente de la LAN, siempre analizado por el IPS en cada una de las conexiones.

A continuación se les mostrara en la Fig. 5.1.3, el diagrama de red de SENCOM, después de la implementación de la zona DMZ.

### Diagrama después de la implementación de la Zona DMZ.

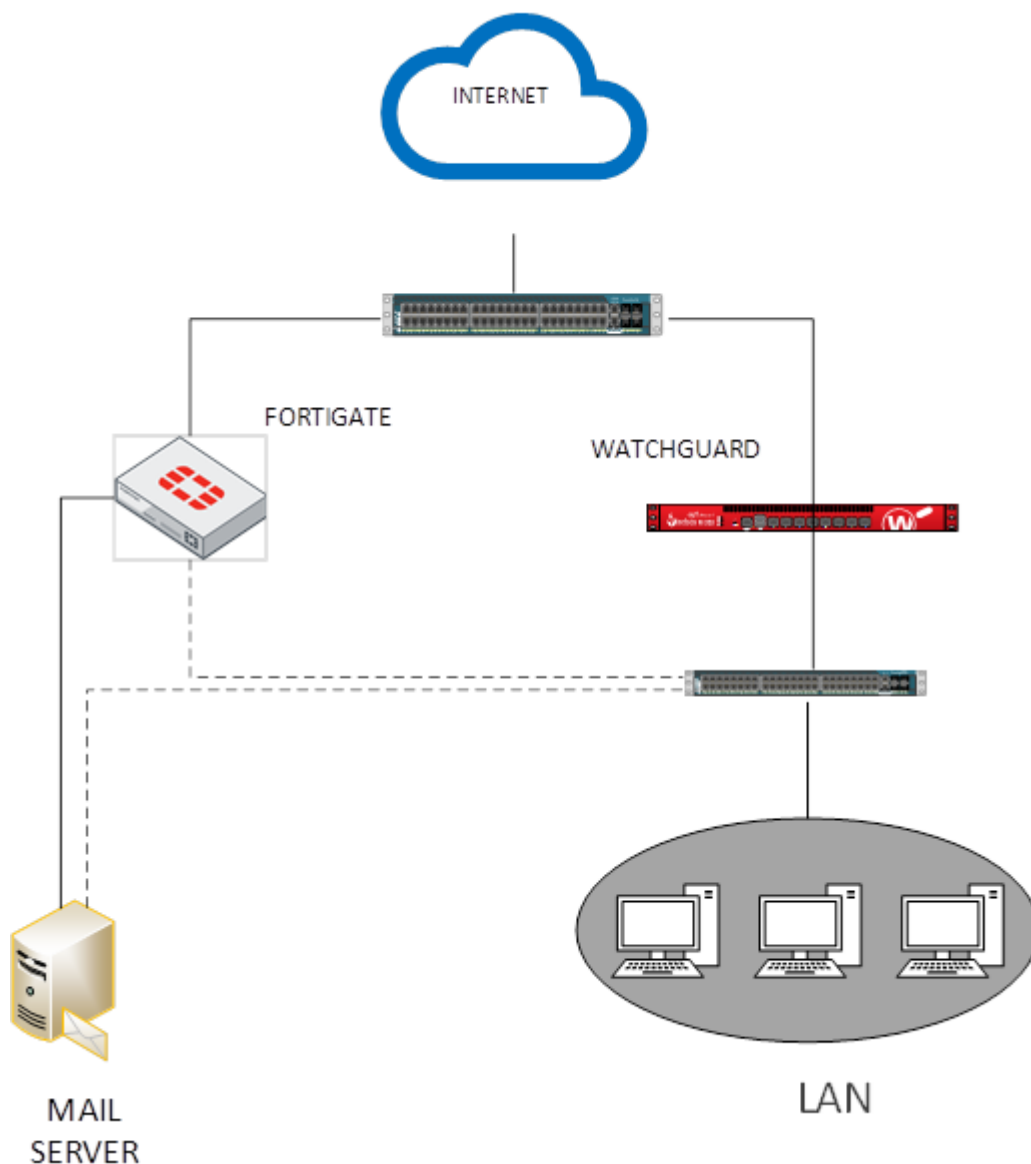


Fig. 5.1.3 Diagrama de red de SENCOM.

A como se puede observar en la nueva topología de red, se utilizó un Fortigate (Fortigate 200D) para la nueva implementación el cual nos estará administrando nuestra zona DMZ.

Fortigate 200D es un next generation firewall (firewall de próxima generación) el cual utiliza procesadores de seguridad especialmente diseñados y servicios de seguridad de inteligencia de amenazas para ofrecer una protección de alto nivel y alto rendimiento, incluido el tráfico encriptado. Fortigate reduce la complejidad con la visibilidad automatizada de las aplicaciones, los usuarios y la red, y proporciona clasificaciones de seguridad para adoptar mejores prácticas en la seguridad.

Debajo de él se observa nuestro web/mail server el cual en este caso lo tenemos ubicado en nuestra zona DMZ. En este caso nuestro servidor de correos es un FORTIMAIL, el cual es el antispam de Fortinet, que nos garantiza una protección especializada y de alta calidad contra amenazas comunes y avanzadas el cual a la vez integra solidas capacidades de protección de datos para evitar la pérdida de estos.

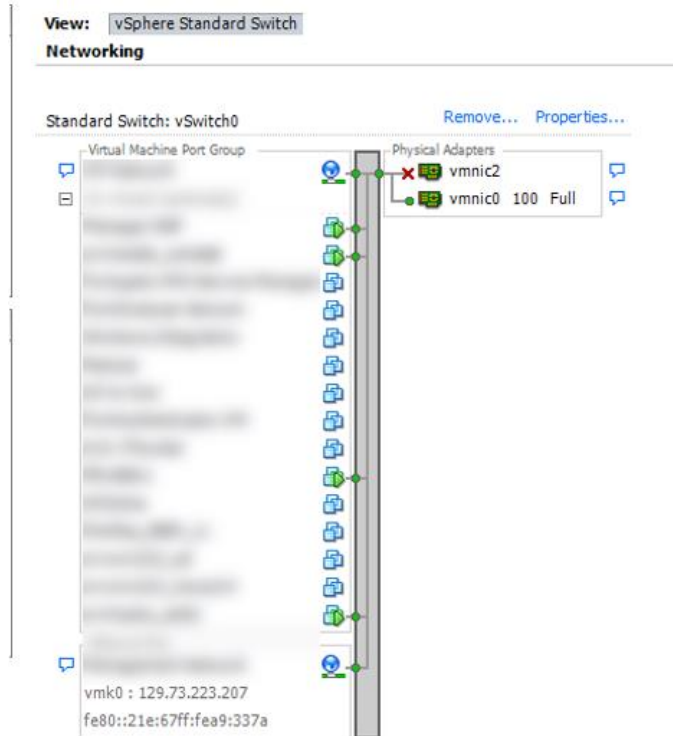
Este Fortimail se encuentra en un ESXi el cual es un ambiente de virtualización que nos permite tener varios hypervisores y una cantidad de interfaces de red disponibles con la facilidad de ser divididas y manejar el tráfico de cada una de ellas por aparte.

Después de haber dejado claro y de describir un poco de los dispositivos de red a utilizar podemos proceder a mostrar el procedimiento seguido para poder crear nuestra DMZ.

Primeramente, se tuvo que crear un Vswitch en nuestro ESXI por donde circulara el tráfico de nuestra DMZ, para esto se siguió el siguiente procedimiento:

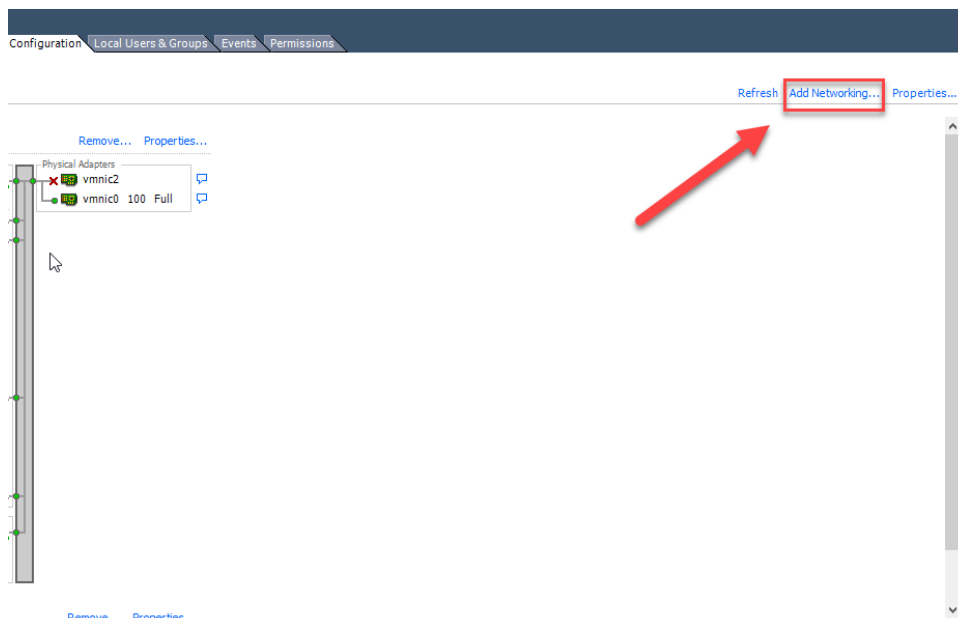
Se accedió a nuestro hypervisor, se pueden observar una cantidad de máquinas saliendo por la interfaz vmnic0, lo cual forma parte de nuestra LAN.

En la Fig. 5.1.4, observamos los primeros pasos para la creación de la interfaz en el ESXI.



**Fig. 5.1.4 Primeros Pasos para la creación de la interfaz en el ESXI.**

Luego se procedió a la creación de nuestra interfaz como se ve en la siguiente Fig. 5.1.5.



**Fig. 5.1.5 Procedimiento para la creación de la interfaz.**



En la Fig. 5.1.6, presentamos el establecimiento de la interfaz de la zona DMZ.

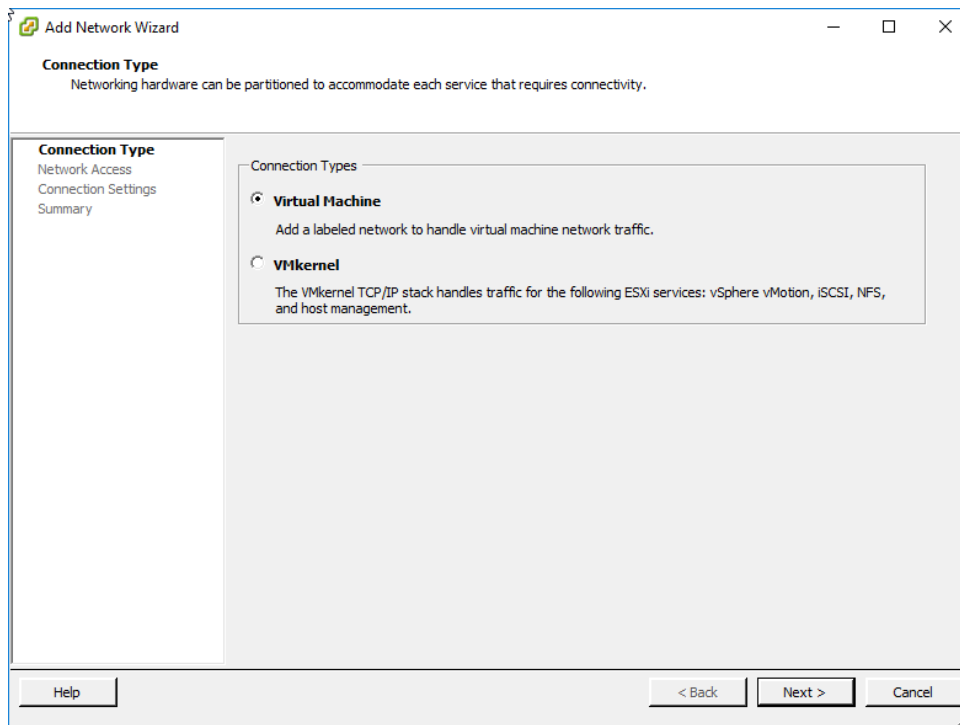


Fig. 5.1.6 Establecimiento de la interfaz de la zona DMZ.

En la Fig. 5.1.7, mostramos la creación de la interfaz de la zona DMZ.

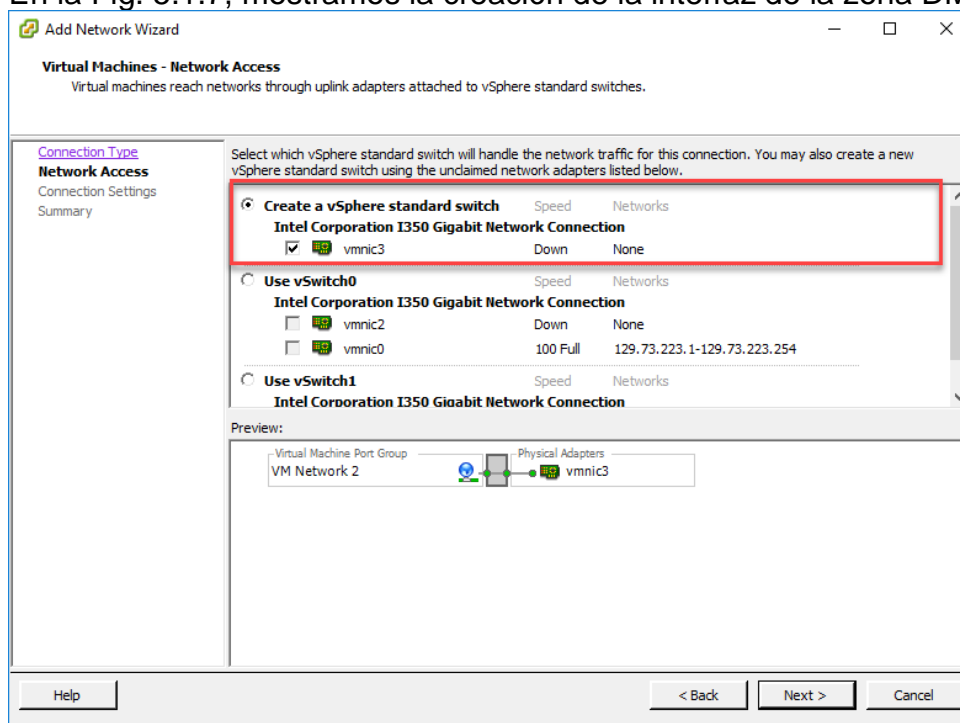


Fig. 5.1.7 Creando la Interfaz de la zona DMZ.

Configurando la zona DMZ lo podemos ver en la siguiente Fig. 5.1.8.

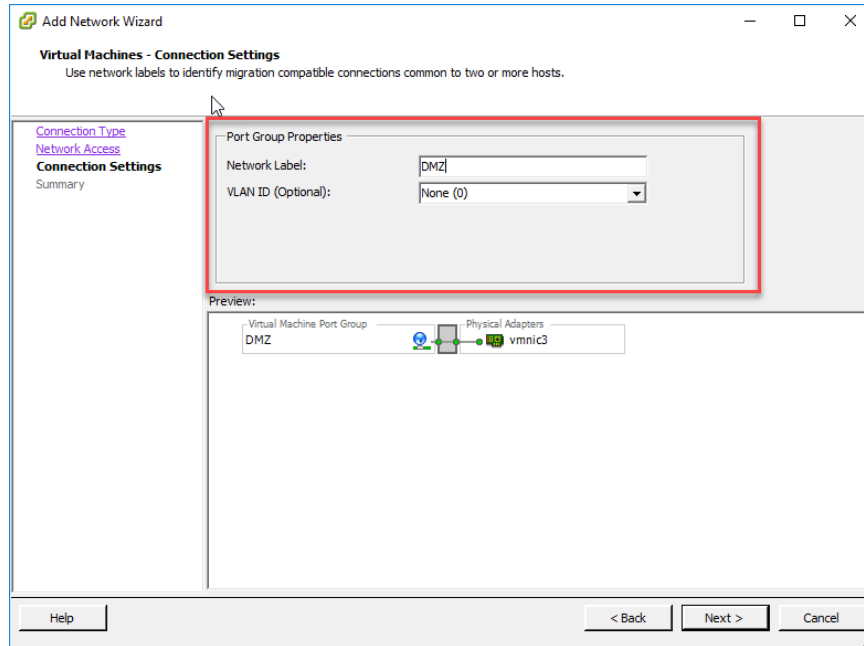


Fig. 5.1.8 Configurando la zona DMZ.

En la Fig. 5.1.9, enseñamos la agregación la interfaz configurada al ESXI.

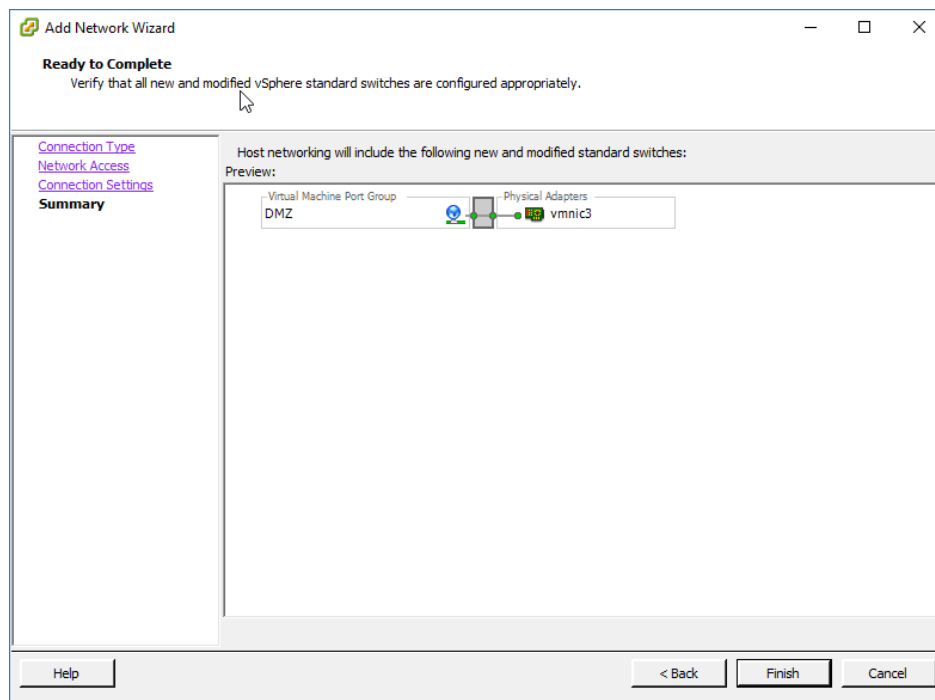


Fig. 5.1.9 Agregando la interfaz configurada al ESXI.

En la Fig. 5.1.10, mostramos el establecimiento de la interfaz del ESXI.



Fig. 5.1.10 Establecimiento de la interfaz del ESXI.

De esta manera tenemos creado nuestro Vswitch, por donde pasará el tráfico de nuestra DMZ, en este servidor se desplegará nuestro Fortimail.

## 5.2. Fortigate:

A como se pudo ver en el grafico anterior el fortigate está conectado directamente a internet pero de igual manera tiene una conexión al swith LAN, por lo cual se le asignó una IP para administración, esta configuración podrá verse en la imagen relacionada con las interfaces de FORTIGATE. [15]

En la Fig. 5.2.1, observamos la plataforma del UTM FortiGate 200 D.

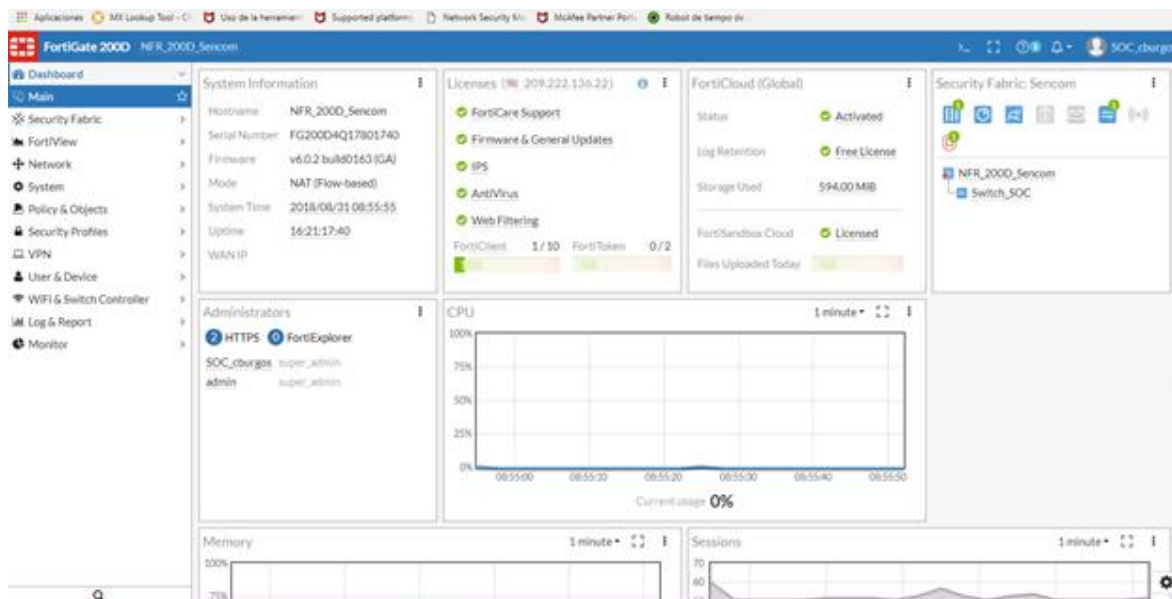


Fig. 5.2.1 Plataforma del UTM FortiGate 200 D para establecer la zona DMZ.

### 5.3. Interfaces:

A continuación estableceremos los puertos del UTM con el direccionamiento IP privado en la siguiente Fig. 5.3.1.

Status	Name	Members	IP/Netmask	Type	Access	Ref.
Physical (10)						
dmz1			10.10.10.1255.255.255.0	Physical Interface	PING HTTPS HTTP FMG-Access CAPWAP	0
dmz2			0.0.0.0.0.0.0	Physical Interface	PING FMG-Access CAPWAP	0
mgmt			192.168.1.99 255.255.255.0	Physical Interface	PING HTTPS SSH HTTP FMG-Access	1
port14 (1 Connected FortiSwitch(s))			Dedicated to FortiSwitch	Physical Interface	PING CAPWAP	4
port15 (Red SENCOM)			129.73.223.219 255.255.255.0	Physical Interface	PING HTTPS SSH HTTP FortiTelemetry	3
port16 (DMZ Sencom)			172.16.30.1 255.255.255.248	Physical Interface	PING	2
wan1 (OUTSIDE_INTERNET)				Physical Interface	PING HTTPS HTTP FMG-Access	6
wan2			0.0.0.0.0.0.0	Physical Interface	PING FMG-Access	0
VLAN Switch (1)						
lan (VLAN ID: 0)			192.168.100.99 255.255.255.0	VLAN Switch (13)	PING HTTPS HTTP FMG-Access CAPWAP	2

**Fig. 5.3.1 Establecimiento de los puertos del UTM con sus direccionamiento IP Privado.**

Se pueden observar las distintas interfaces etiquetadas con la dirección en donde apuntan, en este caso las que nos interesan son:

- Puerto 15 (Red SENCOM)
- Puerto 16 (Red DMZ)
- WAN1 (Outside\_Internet)

A continuación se presentara en la Fig. 5.3.2, la configuración de la interfaz LAN de SENCOM.

**Edit Interface**

Interface Name: port15 (70:4C:A5:10:0C:1B)  
 Alias: Red SENCOM  
 Link Status: Up  
 Type: Physical Interface

Tags: Role: Undefined

Address: Addressing mode: Manual DHCP PPoE  
 IP/Network Mask:

Administrative Access:  
☒ IPv4 ☒ HTTPS ☒ HTTP ☒ PING ☐ FMG-Access  
☐ CAPWAP ☒ SSH ☐ SNMP ☐ FTM  
☐ RADIUS Accounting ☒ FortiTelemetry

☐ DHCP Server

Networked Devices: Device Detection: ☐

OK Cancel

**Fig. 5.3.2 Configuración de la interfaz LAN de SENCOM.**

Estableciendo la configuración del puerto del UTM para la zona DMZ en la Fig. 5.3.3.

The screenshot shows the 'Edit Interface' configuration window for a port named 'port16 (70:4C:A5:10:0C:1C)'. The 'Alias' is set to 'DMZ Sencom'. The 'Link Status' is 'Up' with a green arrow icon. The 'Type' is 'Physical Interface'. Under the 'Tags' section, the 'Role' is set to 'DMZ'. The 'Address' section shows 'Addressing mode' set to 'Manual' and 'IP/Network Mask' set to '172.16.30.1/255.255.255.248'. The 'Administrative Access' section has checkboxes for 'IPv4' protocols: 'HTTPS', 'HTTP', 'CAPWAP', 'SSH', 'RADIUS Accounting', 'PING', 'SNMP', 'FortiTelemetry', 'FMG-Access', and 'FTM'. The 'Networked Devices' section has 'Device Detection' turned off. The 'Miscellaneous' section has 'Scan Outgoing Connections to Botnet Sites' set to 'Disable'. At the bottom are 'OK' and 'Cancel' buttons.

**Fig. 5.3.3 Configuración del Puerto del UTM para la Zona DMZ.**

Como se ve en la Fig. 5.3.4, la configuración del enlace WAN.

The screenshot shows the 'Edit Interface' configuration window for a link named 'wan1 (70:4C:A5:10:0C:0A)'. The 'Alias' is set to 'OUTSIDE\_INTERNET'. The 'Link Status' is 'Up' with a green arrow icon. The 'Type' is 'Physical Interface'. The 'Estimated Bandwidth' section shows '0 kbps Upstream' and '0 kbps Downstream'. Under the 'Tags' section, the 'Role' is set to 'WAN'. The 'Address' section shows 'Addressing mode' set to 'Manual' and 'IP/Network Mask' is empty. The 'Administrative Access' section has checkboxes for 'IPv4' protocols: 'HTTPS', 'HTTP', 'CAPWAP', 'SSH', 'RADIUS Accounting', 'PING', 'SNMP', 'FortiTelemetry', 'FMG-Access', and 'FTM'. The 'Miscellaneous' section has 'Scan Outgoing Connections to Botnet Sites' set to 'Disable' and 'Enable Explicit Web Proxy' turned off. At the bottom are 'OK' and 'Cancel' buttons.

**Fig. 5.3.4 Configuración del enlace WAN con su IP Publica.**

Después de la configuración de las interfaces podemos añadir las direcciones de servidores DNS para la navegación, en este caso a como se verá a continuación se utilizan los DNS de Google.

#### 5.4. Servidores DNS:

En esta parte asignaremos los servidores DNS que ocuparemos se mostrara en la Fig. 5.4.1.

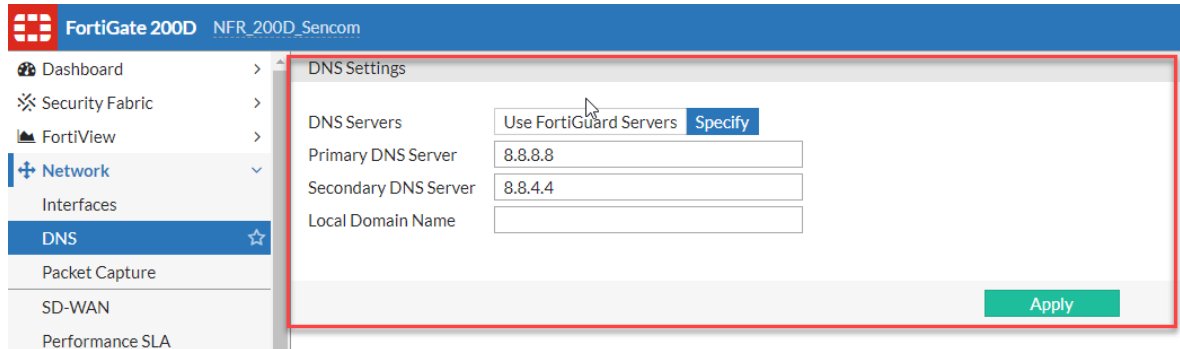


Fig. 5.4.1 Integrando los Servidores Forwarding del DNS de Google.

En esta Fig. 5.4.2, se observa los servidores DNS de Google.

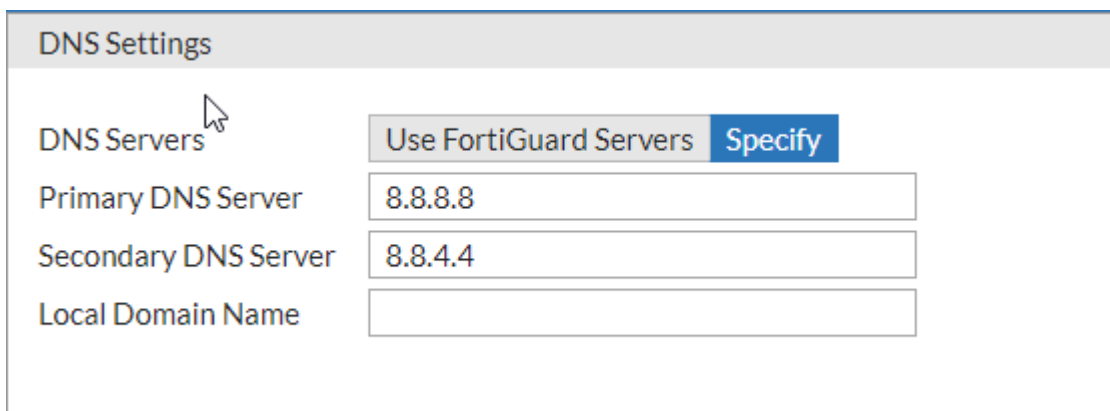


Fig. 5.4.2 Establecimiento de los servidores de DNS de Google.

Ya que tenemos las configuraciones básicas establecidas es hora de hacer nuestra primera configuración de routing, en la cual a como se espera es nuestras rutas de salida a internet

### 5.5. Rutas estáticas:

A continuación haremos el enrutamiento estático del enlace WAN en la siguiente Fig. 5.5.1.

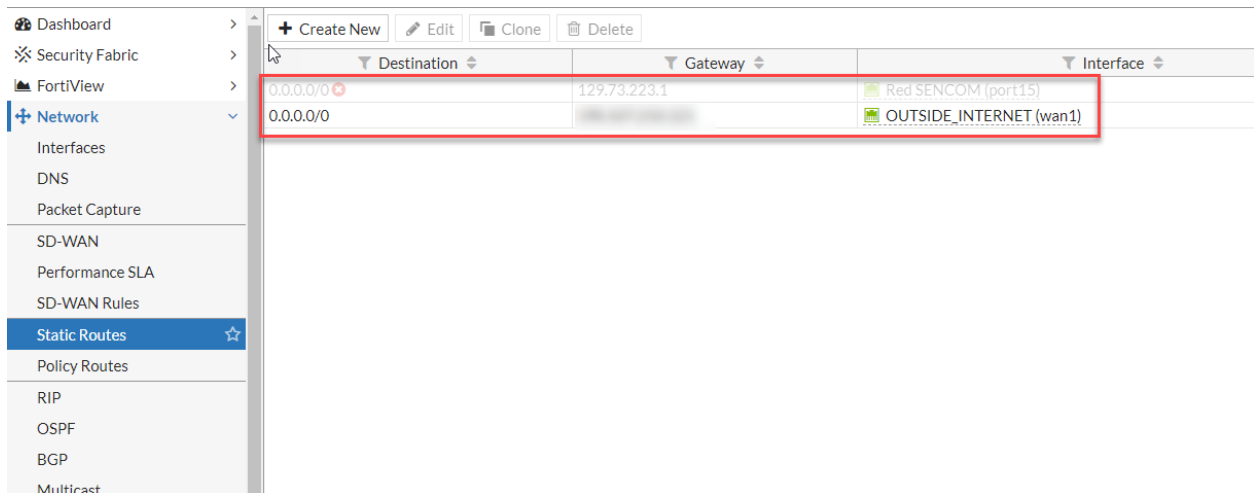


Fig. 5.5.1 Ingresando el Enrutamiento Estático del enlace WAN.

A como se puede observar en nuestra imagen de rutas estáticas, existen dos, una para la salida a internet por nuestro Gateway el cual es directamente nuestra puerta de salida de IP pública (por motivos de seguridad no se presentan las IPs públicas).

En la Fig. 5.5.2, enseñamos la configuración el enrutamiento estático por el enlace WAN.

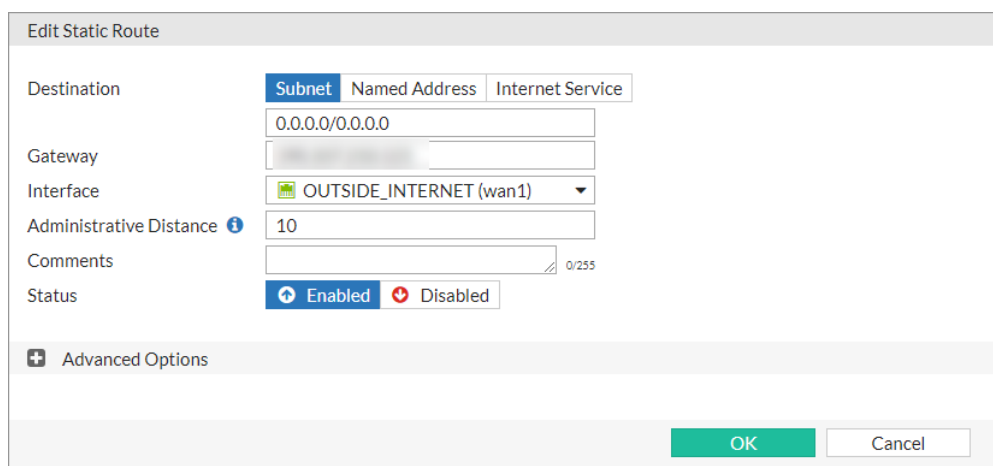


Fig. 5.5.2 Configurando del Enrutamiento Estático por el enlace WAN.

En la Fig. 5.5.3, observamos la configuración del enlace WAN con su enrutamiento estático.

**Fig. 5.5.3 Configuración del enlace WAN con su Enrutamiento Estático.**

Esta segunda imagen es de una ruta redundante, la cual utiliza el Gateway de nuestra LAN, a como se puede ver la distancia administrativa es mayor que nuestro primer enlace, lo cual significa que este actuara solamente si el primero pierde conexión. Debido a que es una DMZ solo lo dejaremos con un enlace y deshabilitamos el segundo con nuestra LAN. [10]

## 5.6. Políticas:

Después de haber realizado el direccionamiento y enrutamiento necesario, es tiempo de ejercer políticas de navegación y por supuesto lo más importante realizar la política que enrute nuestra DMZ con el internet.

En la siguiente Fig. 5.6.1, revelamos el establecimiento de las distintas políticas de red de la empresa SENCOM.

ID	Name	From	To	Source	Destination	Schedule	Service
8	Permisos Web 2	VLAN_LAN (vsw:port14)	OUTSIDE_INTERNET (wan1)	LAN FSW	all	Control Restrictivo	ALL
1	Permisos Web 1	VLAN_LAN (vsw:port14)	OUTSIDE_INTERNET (wan1)	LAN FSW	all	Control de Salida	ALL
7	NAT de Correo	OUTSIDE_INTERNET (wan1)	DMZ Sencom (port16)	all	Mail Service	always	Email Acc Web Acc
6	Salida DMZ	DMZ Sencom (port16)	OUTSIDE_INTERNET (wan1)	all	all	always	ALL
2	Acceso VPN	SSL-VPN tunnel interface (ssl.root)	Red SENCOM (port15)	all SSL-vpn-user	all	always	ALL
5	RED_SENCOM_RED_LAN	Red SENCOM (port15)	lan	all	all	always	ALL
0	Implicit Deny	any	any	all	all	always	ALL

**Fig. 5.6.1 Establecimientos de las distintas políticas de la red de la Empresa SENCOM.**



## 5.7. Salida DMZ:

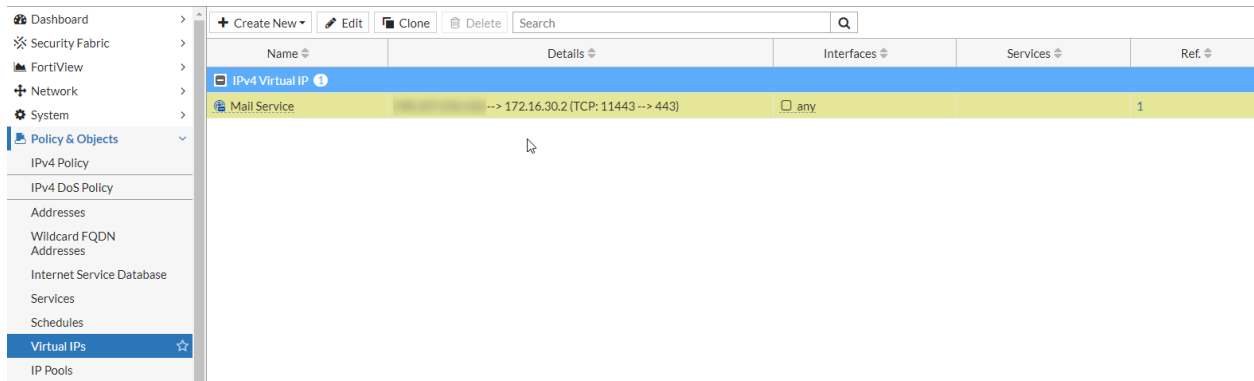
En la siguiente Fig. 5.7.1, mostraremos el establecimiento de la política de la zona DMZ.

The screenshot displays the 'Edit Policy' window for a firewall policy named 'Salida DMZ'. The interface is divided into several sections:

- Policy Configuration:** This section, highlighted with a red border, contains the following settings:
  - Name:** Salida DMZ
  - Incoming Interface:** DMZ Sencom (port16)
  - Outgoing Interface:** OUTSIDE\_INTERNET (wan1)
  - Source:** all
  - Destination:** all
  - Schedule:** always
  - Service:** ALL
  - Action:** ACCEPT (selected), DENY, LEARN
- Firewall / Network Options:** This section, also highlighted with a red border, includes:
  - NAT:** Enabled (toggle on)
  - IP Pool Configuration:** Use Outgoing Interface Address (selected), Use Dynamic IP Pool
  - Security Profiles:**
    - AntiVirus:** Enabled, AV\_Sencom
    - Web Filter:** Disabled
    - DNS Filter:** Disabled
    - Application Control:** Disabled
    - IPS:** Enabled, IPS\_Sencom
    - SSL Inspection:** Enabled, certificate-inspection
  - Logging Options:**
    - Log Allowed Traffic:** Enabled, Security Events, All Sessions
    - Capture Packets:** Enabled
  - Comments:** Write a comment... (0/1023)
  - Enable this policy:** Enabled (toggle on)
- Summary / Statistics:** Located on the right side, showing:
  - ID:** 6
  - Last used:** 23 minute(s) ago
  - First used:** 2 day(s) ago
  - Hit count:** 433
  - Active sessions:** 3
  - Total bytes:** 820.82 kB
  - Current bandwidth:** 0 B/s
  - Online Help:** Link available

Fig. 5.7.1 Establecimos la política de la Zona DMZ.

A continuación en la Fig. 5.7.2, observamos la configuración de la política de NAT, en este caso su utilizara un SNAT para después agregarlo a una política.



**Fig. 5.7.2 Configurando las políticas del NAT**

Aquí se hará la configuración necesaria para garantizar el acceso a nuestro servidor desde fuera de nuestra LAN, en donde se especifican la IP externa con la IP que será dirigido y el puerto que se utilizara para el acceso a este servicio, en este caso se destinó el puerto 11443 como externo y será redirigido al puerto 443 el cual pertenece a HTTPS.

En la Fig. 5.7.3, presentamos el establecimiento del SNAT para la zona DMZ.

**Edit Virtual IP**

Name: Mail Service  
Comments: NAT de Correo  
Color: Change

**Network**

Interface: any  
Type: Static NAT  
External IP Address/Range: [ ] - [ ]  
Mapped IP Address/Range: 172.16.30.2 - 172.16.30.2

Optional Filters: ☐

Port Forwarding: ☒

Protocol: TCP UDP SCTP ICMP  
External Service Port: 11443 - 11443  
Map to Port: 443 - 443

OK Cancel

**Fig. 5.7.3 Estableciendo el SNAT para la utilización de la Zona DMZ.**

Luego podemos agregar nuestro NAT a nuestra política como se ve en la Fig. 5.7.4.

**Edit Policy**

**Name** NAT de Correo

**Incoming Interface** OUTSIDE\_INTERNET (wan1)

**Outgoing Interface** DMZ Sencom (port16)

**Source** all

**Destination** Mail Service

**Schedule** always

**Service** Email Access, Web Access

**Action** ACCEPT, DENY, LEARN

**Firewall / Network Options**

**NAT** ON

**Security Profiles**

Antivirus: AV default

Web Filter: OFF

DNS Filter: OFF

Application Control: OFF

IPS: protect\_email\_server

SSL Inspection: certificate-inspection

**Logging Options**

Log Allowed Traffic: Security Events, All Sessions

Capture Packets: ON

Comments: Write a comment... 0/1023

Enable this policy: ON

**Summary / Statistics**

ID: 7

Last used: 32 minute(s) ago

First used: 2 day(s) ago

Hit count: 73

Active sessions: 0

Total bytes: 1.44 MB

Current bandwidth: 0 B/s

[Online Help](#)

Fig. 5.7.4 Agregando el NAT a las políticas de la red.

## 5.8. Fortimail:

Después de haber mostrado toda la configuración necesaria en nuestro enrutador de perímetro (Fortigate), nos falta la instalación y configuración de parte de nuestros servidor que estará localizado en nuestra DMZ.

A continuación se ve en la Fig. 5.8.1, la configuración del Fortimail de SENCOM.

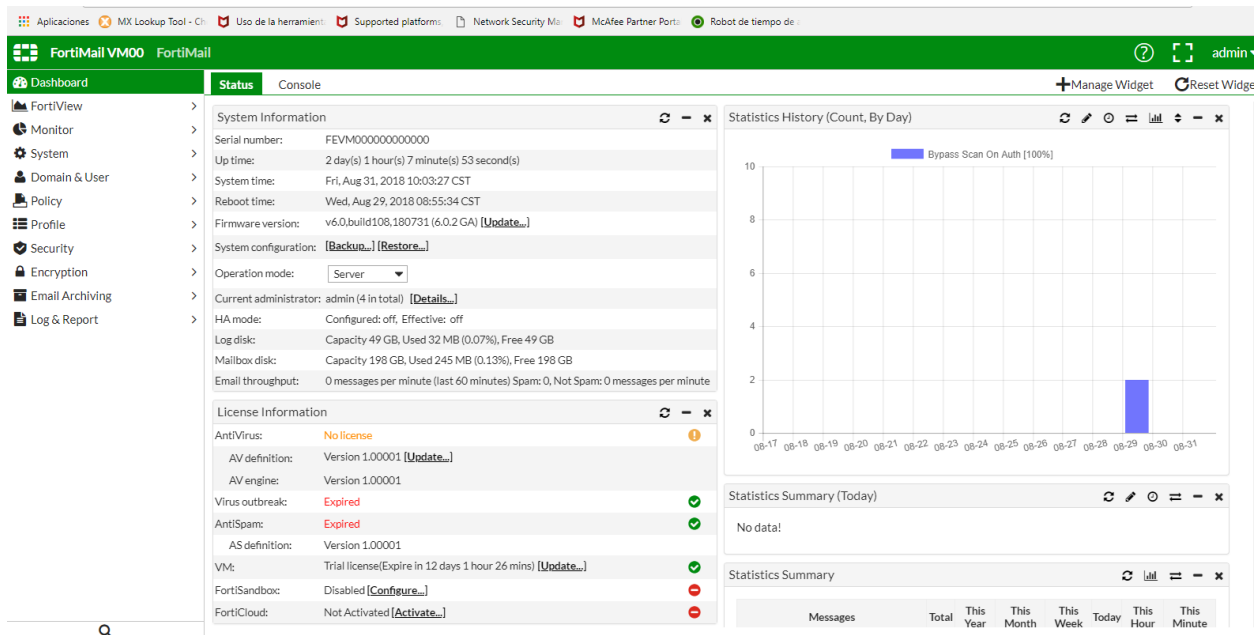
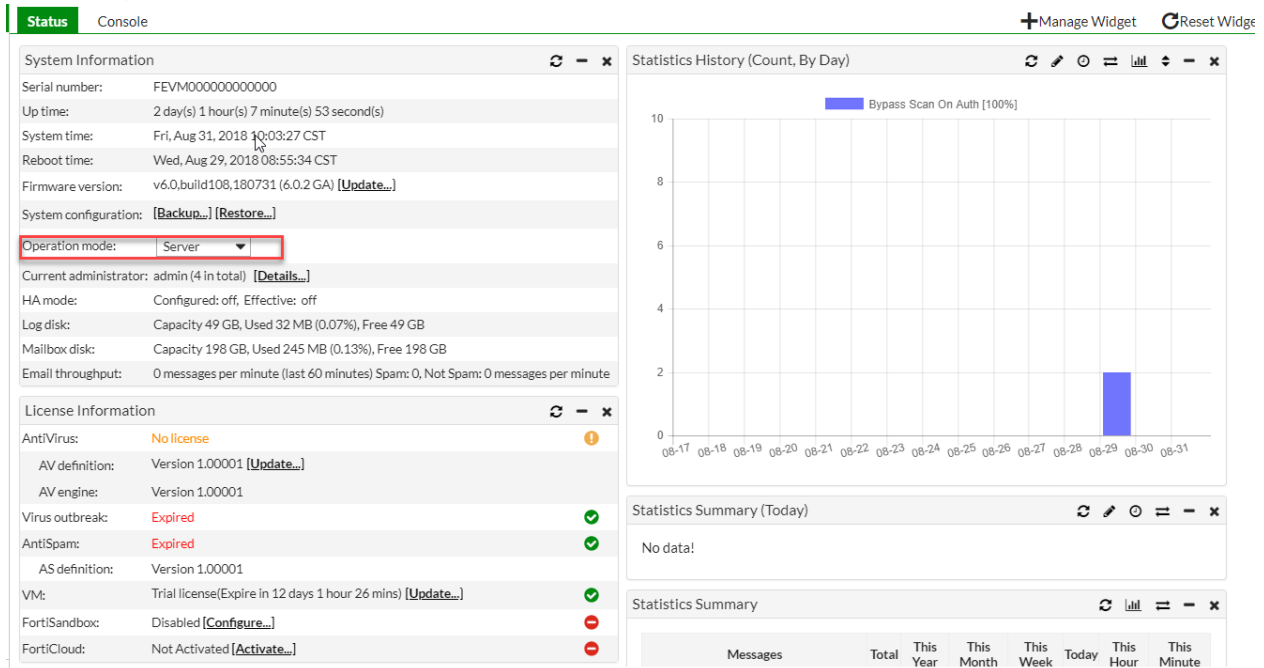


Fig. 5.8.1 Configuración del Fortimail de SENCOM.

A como se había mencionado anteriormente, el modo en el cual operaremos nuestro Fortimail será el modo server, ya que consta con las características necesarias que satisfacen el fin requerido. Este Servidor Fortimail está en el capítulo anterior todas las configuraciones debidas.

En la Fig. 5.8.2, veremos el modo de operación del Fortimail.



**Fig. 5.8.2 Modo de Operación del Fortimail.**

Es necesaria la configuración de interfaces en el fortimail:

Algo antes no mencionado es de que este servidor tendrá dos interfaces de red, una de ellas será con su IP de web server el cual estará localizado en la DMZ y la otra será una IP administrativa la cual se conectara a nuestro switch LAN ( esto se puede observar en nuestro diagrama final de red DMZ).

En la Fig. 5.8.3, observamos el establecimiento del interfaz del Fortimail.

Link Status	Name	Type	IP/Netmask	IPv6/Netmask	Access	
✓	port1	Physical	129.73.223.225/24	::/0	HTTPS,PING,SSH	●
✓	port2	Physical	172.16.30.2/29	::/0	HTTPS,PING	●

**Fig. 5.8.3 Establecimiento del interfaz del Fortimail.**

En la siguiente Fig. 5.8.4, mostramos la configuración de la interfaz con los distintos protocolos de red.

The screenshot shows the 'Edit Interface' window for 'port1 (00:0c:29:17:34:2c)'. The 'Link status' is 'Up'. Under 'Addressing Mode', 'Manual' is selected with IP/Netmask '129.73.223.225 / 24' and IPv6/Netmask ':: / 0'. Under 'Advanced Setting', 'Access' has HTTPS, PING, and SSH checked, while SNMP, HTTP, and TELNET are unchecked. 'Web access' has Admin and Webmail checked. 'Mail access' has POP3, IMAP, POP3S, and IMAPS checked. The MTU is set to 1500, and the 'Administrative status' is 'Up'. 'OK' and 'Cancel' buttons are at the bottom right.

**Fig. 5.8.4 Configurando la interfaz y permitiendo los distintos protocolos de red.**

En la Fig. 5.8.5, enseñamos el establecimiento de la interfaz del Fortimail.

The screenshot shows the 'Edit Interface' window for 'port2 (00:0c:29:17:34:36)'. The 'Link status' is 'Up'. Under 'Addressing Mode', 'Manual' is selected with IP/Netmask '172.16.30.2 / 29' and IPv6/Netmask ':: / 0'. Under 'Advanced Setting', 'Access' has HTTPS, PING, and IMAP checked, while SNMP, HTTP, TELNET, and SSH are unchecked. 'Web access' has Webmail checked, and 'Admin' is unchecked. 'Mail access' has POP3, IMAP, POP3S, and IMAPS checked. The MTU is set to 1500, and the 'Administrative status' is 'Up'. 'OK' and 'Cancel' buttons are at the bottom right.

**Fig. 5.8.5 Estableciendo la interfaz del Fortimail.**

De igual manera se tendrán que configurar servidor DNS en nuestro FORTIMAIL, usaremos los de Google.

En la Fig. 5.8.6, observamos el ingreso de los servidores DNS en el Fortimail.

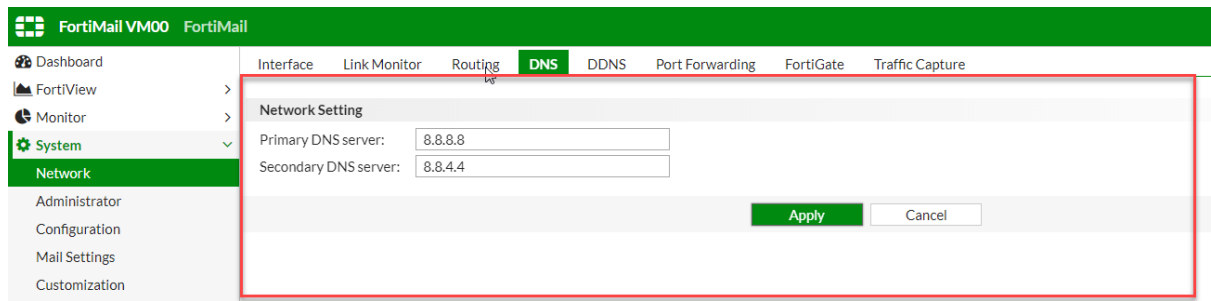


Fig. 5.8.6 Ingresando los Servidores DNS de Google.

## 5.9. Routing:

En nuestro Fortimail será necesario realizar la configuración de dos rutas estáticas, una para la comunicación con la administración del mail server y la otra para la salida por medio de su Gateway.

En la Fig. 5.9.1, presentamos el enrutamiento estático del Fortimail.

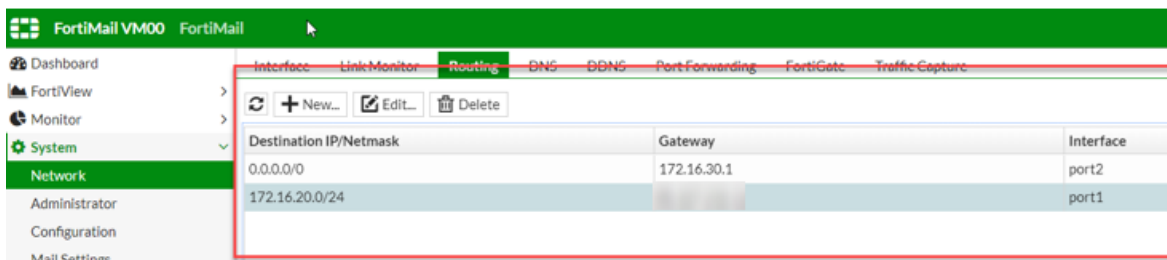


Fig. 5.9.1 Enrutamiento Estático del Fortimail.

En la Fig. 5.9, mostramos el enrutamiento del Fortimail.

The screenshot shows the 'Edit Routing Entry' window in FortiMail. It contains the following fields:

- Destination IP/netmask: 0.0.0.0 / 0
- Interface: port2
- Gateway: 172.16.30.1

At the bottom right, there are 'OK' and 'Cancel' buttons.

Fig. 5.9.2 Mostrando el enrutamiento del Fortimail.

A continuación podremos ver la configuración de políticas por default de nuestro servidor, en esta parte no se ha editado nada ya que son configuraciones empresariales adaptables al entorno y las necesidades, en donde son necesarias políticas de seguridad y el monitoreo de la entrada y salida de correo.

En esta Fig. 5.9.3, observamos el establecimiento de las políticas del Fortimail.

The screenshot shows the 'IP Policy' configuration page in FortiMail. The left sidebar shows the navigation menu with 'Policy' selected. The main content area displays a table of IP policies.

Enabled	ID	Source	Destination	Session
<input checked="" type="checkbox"/>	1	0.0.0.0/0	0.0.0.0/0	<a href="#">Inbound_Session</a>
<input checked="" type="checkbox"/>	2	::/0	::/0	<a href="#">Inbound_Session</a>

Fig. 5.9.3 Estableciendo las políticas del Fortimail.



En la Fig. 5.9.4, enseñamos establecimiento de la política de entrada del Fortimail.

Inbound								
<div> <div> <div>New...</div> <div>Edit...</div> <div>Delete</div> <div>Move</div> <div>Policy Lookup...</div> </div> <div> <div>1 / 1</div> <div>Records per page: 50</div> <div>Domain: --All--</div> <div>Show system policy</div> </div> </div>								
Enabled	ID	Domain Name	Sender Pattern	Recipient Pattern	AntiSpam	AntiVirus	Content	Resource
<input checked="" type="checkbox"/>	1	system	*@*	*@*	AS_Inbound	AV_SysQuarantine	CF_Inbound	Res_Default

**Fig. 5.9.4 Establecimiento de la política de entrada del Fortimail.**

En esta Fig. 5.9.5, exhibimos el establecimiento de la política de salida del Fortimail.

Outbound								
<div> <div> <div>New...</div> <div>Edit...</div> <div>Delete</div> <div>Move</div> <div>Policy Lookup...</div> </div> <div> <div>1 / 1</div> <div>Records per page: 50</div> <div>Domain: --All--</div> <div>Show system policy</div> </div> </div>								
Enabled	ID	Domain Name	Sender Pattern	Recipient Pattern	AntiSpam	AntiVirus	Content	
<input type="checkbox"/>	2	system	*@*	*@*	AS_Outbound	AV_Reject	CF_Outbound	

**Fig. 5.9.5 Establecimiento de la política de salida del Fortimail.**

De esta manera se tiene configurada nuestra DMZ, alejada de nuestra red LAN e inclusive con otro direccionamiento de salida, para poder tener acceso a nuestro servicio desde internet es necesario digitar: [https://<ip\\_externa>:1433](https://<ip_externa>:1433) (puerto establecido en nuestra configuración al igual que el protocolo https)

Por los momentos es de uso interno empresarial por lo cual los usuarios añadidos tienen credenciales específicas para la utilización del servicio.

## Conclusiones.

En esta monografía aplicamos toda la base teórica y práctica precisamente para tener una mayor seguridad en la red de la compañía Systems Enterprise S.A. Durante todo el proceso de instalación y configuración de: (IPS, UTM, DNS, Fortimail y una Zona DMZ). Obtuvimos los resultados satisfactorios cumpliendo con los objetivos planteados en cada uno de estas implementaciones antes mencionadas.

Concluimos que es necesario implementar estas soluciones de seguridad con sus mejores prácticas y políticas en una organización porque los ataques cibernéticos están teniendo el mayor éxito en el eslabón más débil y difícil de proteger, en este caso son los usuarios, se trata de uno de los factores que han incentivado el número de ataques internos. No importando los procesos y la tecnología, finalmente el evitar los ataques queda en manos de nosotros los administradores de red. Esta solución integral busca proteger, solucionar y evitar las distintas vulnerabilidades. Esto fue nuestra meta principal de este documento en organizar y establecer nuevas soluciones de seguridad en la red de la empresa Systems Enterprise S.A.

Nosotros recomendamos estar al día de la aparición de nuevas técnicas que amenazan la seguridad de su red o equipo informático, para tratar de evitarlas o de aplicar la solución más efectiva posible. Navegue por páginas web seguras y de confianza. Para diferenciarlas identifique si dichas páginas tienen algún sello o certificado que garanticen su calidad y fiabilidad. No ingresar datos personales y contraseñas en cualquier página Web. También no abrir correos remitentes desconocidos porque dentro del contenido puede llevar un enlace para ser redirigido, Cambiar las contraseñas más frecuentemente y tener un doble patrón de autenticación en sus cuentas personales. Otro punto es encriptar todos los discos duros de las computadoras con el objetivo de prevenir las pérdidas de datos.

## Bibliografía:

- [1] A.FOROUZAN, B. ((2002)). *TRANSMISION DE DATOS Y REDES DE COMUNICACIONES*. Madrid: McGrawHill.
- [2] Andina, F. (2014). *REDES ADMINISTRACION DE SERVIDORES*. Buenos Aires.
- [3] B., K. A. (2013). *Hacking Etico 101*.
- [4] Barker, K. &. (s.f.). *CCNA Security 640-554*. 800 East 96 th Street Indianapolis,IN 46240: Pearson Education,Inc.
- [5] CISCO. (2018). *Curricula de CCNA del Modulo 1-4*.
- [6] Fortinet. (s.f.). *Download Firmware*. Obtenido de <https://support.fortinet.com/Download/FirmwareImages.aspx>
- [7] Fortinet. (s.f.). *Recurso de Fortimail*. Obtenido de <https://docs.fortinet.com/fortigate/admin-guides>
- [8] Garcia Rambla, J. L. (2017). *Ataques en redes de datos IPV4 e IPV6*. España, tercera edición revisada y ampliada.
- [9] Huerta, A. V. (Julio, 2002). *SEGURIDAD EN UNIX Y REDES*.
- [10] James O. Coplien, R. C. (2012). *Código Limpio*. Madrid, España.: ANAYA.
- [11] M Carling, S. D. (s.f.). *Guia Avanzada Administracion de Sistemas Linux*. Madrid, Mexico: Prentice Hall.
- [12] Marchionni, E. A. (s.f.). *ADMINISTRADOR DE SERVIDORES. USERS*.
- [13] McAfee. (s.f.). *McAfee Network Security Platform*. . Obtenido de <https://community.mcafee.com/t5/Network-Security-Platform-NSP/bd-p/network-security-platform-expert-center>
- [14] Syed M.Sarwar, R. K. (s.f.). *El Libro de Unix*. Madrid: Addison Wesley.
- [15] TANENBAUM, A. S. (2012). *Redes de Computadoras*. Mexico: PEARSON.
- [16] Tori, C. (2008). *Hacking Etico*. Buenos Aires, Argentina.
- [17] Zemánek, J. (2004). *CRACKING SIN SECRETOS*. RA~MA.
- [18] Zentyal. (s.f.). *Zentyal.org Documentacion para el servidor DNS*. Obtenido de <https://doc.zentyal.org/es/>

## Anexos:

### Anexo 1. Diagrama Final de SENCOM

En la Fig. 1A.1 observamos el diagrama de la red de computadora de la empresa SENCOM al completar todos nuestros objetivos.

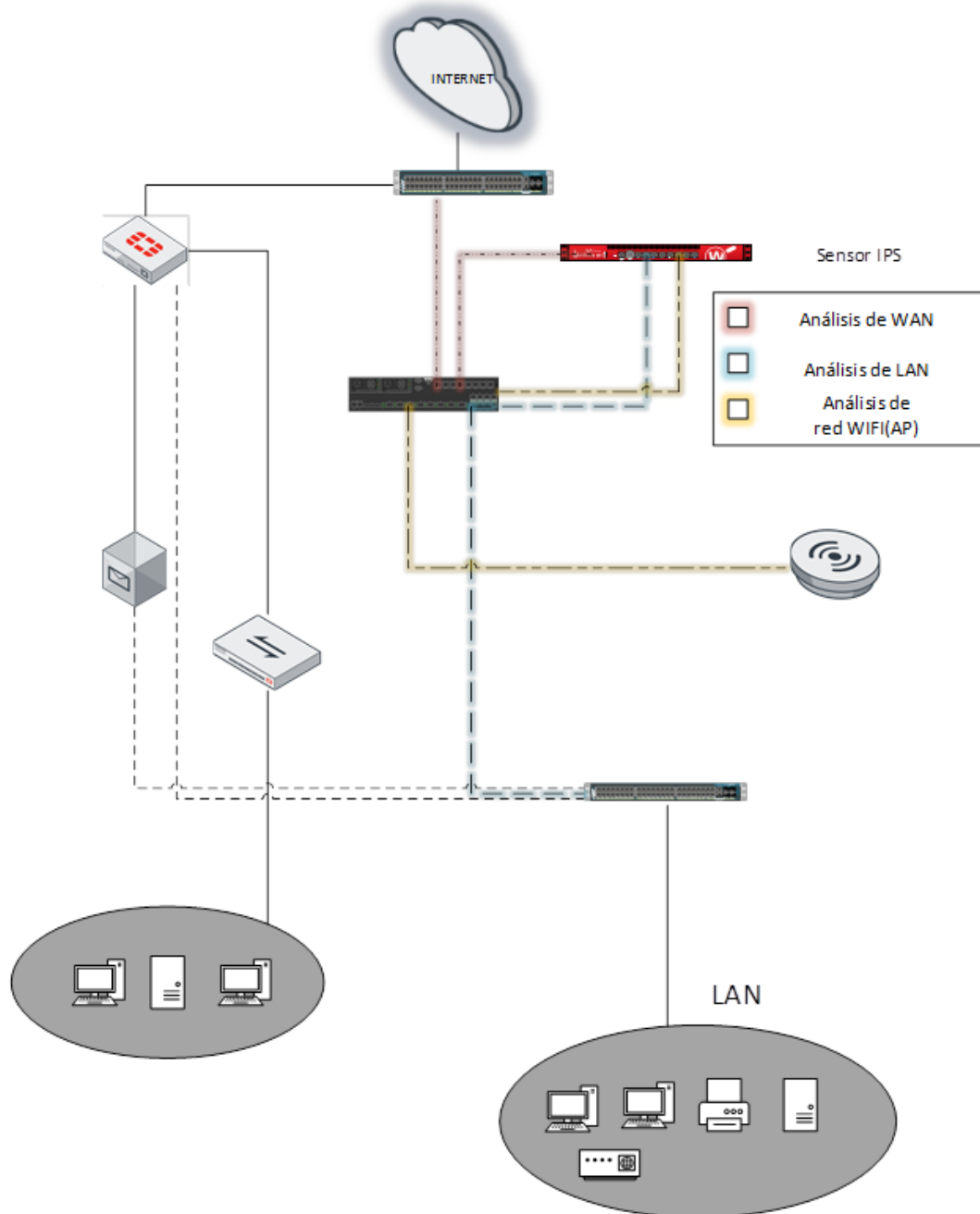


Fig. 1A.1 Diagrama de la red SENCOM

## ANEXO 2. Tabla de Cotizaciones

Marca	Precio en Dólares.
UTM Fortinet Fortigate 200 D	\$ 3,837.32
UTM WatchGuard M-200	\$ 6,500
8 PATCHCORD 7FT CAT 5E GRIS	\$ 2.29
Sensor del IPS M-1450	\$2,000
<b>Total</b>	<b>\$12,355.64</b>

En esta tabla se observan todos los equipos de red que utilizamos para llevar a cabo este proyecto de organización y estructuración de la red que la Empresa SENCOM nos facilitó para hacer esta monografía. Estos precios vienen incluido con IVA y Envío desde el lugar del fabricante.